X-Sieve: CMU Sieve 2.2
Date: Tue, 21 Dec 2004 09:04:04 -0500
To: DraftFips201@nist.gov
From: "Tice F. DeYoung" <tdeyoung@mail.hq.nasa.gov>
Subject: Comments on Public Draft FIPS 201
Cc: Tice.DeYoung-1@nasa.gov, Helen Euler <Helen.L.Euler@nasa.gov>,
Scott Santiago <Scott.Santiago@nasa.gov>
X-MailScanner:
X-MailScanner-From: tdeyoung@mail.hq.nasa.gov

To Whom It May Concern,

The purpose of this email is to officially submit the attached combined NASA comments on the 8 November '04 Public Draft of NIST FIPS 201.

Respectfully Submitted,
Tice F. DeYoung
Special Assistant to NASA CIO for IT Security


FIPS201-Cmts-NASA-TFD.xls

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	NASA	Tice DeYoung	G	Section 2.2 pg. 5 and all subsequent sections in which item is mentioned	What exactly is the Authorizing Official doing in order to "approve" a PIV request. Of all the roles this one is the most vague and seems superfluous. Looking at the wokflow, the Authorizing Official acts as a pass through from Requester to RA and Issuing Authority.	Eliminate the Authorizing Official role or explain what is involved in authorizing a request.
2	NASA	Tice DeYoung	G	Section 2.2.1, 2nd paragraph, 2nd bullet, pg. 5	What is meant by a parent organization? Is this the agency that the person will be working for?	Clarify the meaning.
3	NASA	Tice DeYoung	G	Section 2.2.1, Table 2-2, Level1, pg. 6	Doesn't the requirement to verify the proffered identity documents mean that every federal agency must now have access to multiple databases, including at a minimum the motor vehicle database of all 50 states? Have the states given approval for this? Has any consideration been given to the cost of	Need to identify the issues & costs for implementing this requirement and consider other options.
4	NASA	Tice DeYoung	G	Section 2.2.1, 1st paragraph after Table 2-2, 2nd bullet, pg. 7	The Registration Authority (RA) is required to keep a copy of the identity source documents. If the person is already a Federal employee, most (all?) agencies don't allow photocopying if their identity badges.	Re-write this so that the RA hand copies those portions of the documents that are necessary to verify the identity of the applicant.
5	NASA	Tice DeYoung	G	Section 2.2.1, 1st paragraph after Table 2-2, 2nd bullet, pg. 7	The RA is required to keep a copy of the identity source documents. What steps will be taken to ensure that they are not subsequently used in identity theft, that is, are there specific steps to be taken by the	Identify how documents will be protected.
6	NASA	Tice DeYoung	G	Section 2.3, 1st paragraph pg. 7	How will the copies of the identity source documents be transmitted from the RA to the Authorizing Official (AO) and from the AO to the Issuing Authority (IA)? If they are transmitted electronically, will the copies	State how the documents will be tramsmitted and the security mechanisms used to protect them.

D = Document,1 = FIPS201, 2 = SP800-73

T=Type of Comment, E = editoral, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
7	NASA	Tice DeYoung	G	Section 2.3, 2nd paragraph pg. 7	Because the IA will not be keeping a copy of the identity source documents, how will they dispose of them? As stated above, these can easily be used for identity theft, so they must be adequately disposed of.	State what the IA will do with the coopies of the identity source documents.
8	NASA	Tice DeYoung	G	Section 3.2.1, 5th bullet, pg. 11	Will the PIV card status and registration records be retained as part of the applicants permanent file? If not, what is the retention	State if they will be part of the applicants permanent record.
9	NASA	Tice DeYoung	G	Section 3.2.3, 2nd bullet, pg. 12	The time frame for implementing this has been specified as October 2005, or the beginning of U.S. Government Fiscal Year (FY) 2006. The agencies have already submitted their FY 2006 budgets, so what will OMB be reviewing in the way of PIV system budgets and operational procedures until FY 2007> Will they be doing passbacks because agencies didn't include PIV budgets	Provide information on OMB's intentions to the agencies.
10	NASA	Tice DeYoung	E	Section 3.3.1, 1st paragraph, pg. 14	The acronym ICC is used for integrated circuit chip; whereas in SP 800-73 ICC stands for integrated circuit card (*see Section 2.2, page 11)*. This double use will cause confusion. This acronymn is used in	Edit the document(s) for consistency.
11	NASA	Tice DeYoung	T	Section 4 and sub-sections to 4.4.6, pgs. 17-38	There is barely enough space on a 64 kilobit smart card to store the OS, the applets, the biometric data, the cryptographic functions and the optional data on the card. This will result in a re-badging effort for Federal employees and on-site contractors every two to three years when their PKI certificates expire. How will this be handled in such a way that it does not put an undue financial	Ensure that the old data can be stored elsewhere and expunged from the cards. The PKI applications must be able to get to the stored data for access to archived encryption keys.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
12	NASA	Tice DeYoung	T	Sections 4.1 to 4.4 and sub-sections pgs. 17-38	The PIV card specifications described here exceed those of the newly developed Government Smart Card Interoperability Specification (GSC-IS) version 2.1. Homeland Security Presidential Directive number 12 states that the PIV card standard shall be used by all Federal agencies beginning in October 2005. Their will not be any products out that meet these	Revise the PIV card specification so that it is equivalent to GSC-IS 2.1. Work closely with the IGSA neragency Advisory Board on Smart Cards to develop a transition plan to the additional specifications .
13	NASA	Tice DeYoung	T	Sections 4.1 to 4.4 and sub-sections pgs. 17-38	NASA has initiated a Common Badging and Access Control System (CBACS) that meets GSC-IS 2.1. We are implementing software and processes that provide personal identity verification and validation that are consistent with the identity verification part of FIPS-201, but cannot provide those features that are not included in the extant GSC-IS 2.1. The CBACS has required significant cost expenditures to modify the NASA security infrastructure in terms of hardware, software and a common NASA badging system. However, the FIPS-201 requirement for biometric capture, biometric processing and card datamodel go beyond GSC-IS 2.1 and	Revise the PIV card specification so that it is equivalent to GSC-IS 2.1. Also, work closely with the IGSA neragency Advisory Board on Smart Cards to develop a transition plan for the additional specifications.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
14	NASA	Tice DeYoung	T	Section 4.1, 2nd paragraph pg. 17	The PIV cards must comply with ISO/IEC 7810, 7816 and 10373 for the contact card characteristics. Before the PIV cards are promulgated across the federal government, a detailed study of the strength of these cards must be undertaken. There are companies that will take a smart card and perform a number of tests on it to determine the ease or difficulty of stealing the access codes from the card. In discussions with them, they stated that they had never failed to break every smart card they had ever tested. However, they said that gaining the	NASA strongly recommends that one or more of these companies be hired to perform these tests on the smart cards prior to their use across the Federal government.
15	NASA	Tice DeYoung	T	Section 4.1.4, Figure 4-1, pg. 19	There is no mention of a holographic image on the front of the card. This technique is used effectively by a number of states to discourage forgeries. This should also be used here as an added deterrent to would be	Add a holographic image as one of the mandatory items on the front of the PIV card.
16	NASA	Tice DeYoung	T	Section 4.1.4, Figure 4-1, Zone 3, pg. 19	The cardholder's signature on the front of the card should be mandatory, not optional.	Make the signature a mandatory item.
17	NASA	Tice DeYoung	T	Section 4.1.4, Figure 4-1, Zones 4 & 5, pg. 19	Putting the pay grade or the rank of the cardholder on the card guarantees that a significant percentage of duplicate cards will have to be made every year when one of these fields change while everything else	Do not allow either the pay grade or the rank on the front of the card.
18	NASA	Tice DeYoung	T	Section 4.1.4, Figure 4-1, Zones 9 & 10, pg. 19	Why is United States Government mandatory and the agency name optional? The agency name should be mandatory.	Make the agency name mandatory and USG optional.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
19	NASA	Tice DeYoung	T	Section 4.1.4, Figure 4-1, Zones 9 & 10, pg. 19	Why is it possible to have both United States Government and the agencies name on the PIV card? The mandatory agency name should be sufficient. Having both would clutter the template and could cause some	Only allow one or the other on the PIV card.
20	NASA	Tice DeYoung	T	Section 4.1.4, Figure 4-1, Zone 14, pg. 19	The issue date of the card should be mandatory. The expiration date doesn't belong on the card, but in the agency's personnel database.	Make the issue date mandatory and remove the expiration date.
21	NASA	Tice DeYoung	E	Section 4.1.5.1, 1st paragraph, 1st bullet and 4.1.6.1, 1st & 2nd paragraphs,	The term PIN is confusing because it refers to both the numerical PIN needed for physical access described in Section 3.3. However, here it seems to mean the password required for unlocking the device	Change the language so that it is obvious where PIN is meant and where password is meant.
22	NASA	Tice DeYoung	T	Section 4.1.6.1, 1st & 2nd paragraphs, pg. 24	What is the length requirement for the PIN and for the password? The reference to FIPS PUB 140-2, level 3 indicates that a 6 digit numerical PIN will suffice. This is far below what NIST recommends in its FIPS-112 high level of security.	Discriminate between PIN for physical access and password for logical access. Six numberic digits for the PIN is sufficient. The password, however, should be 6-8 characters in lenght, with at least one each from upper and lower
23	NASA	Tice DeYoung	T	Section 4.1.6.1, all paragraphs, pg. 24	If the PIN pad device activates the PIV card, does this mean that all of the physical access points will have to have both contact and contactless readers? Does this also mean that every physical access device must be part of the agencies information technology security solution, that is, behind the firewall(s) because the PIN activiates the logical access	It the PIN pad device does activate the logical access part of the PIV card, then the physical access device and PIN pad device must be behind the firewall. If it doesn't, then change the language so that it is obvious where PIN is meant and where password is meant.

D = Document,1 = FIPS201, 2 = SP800-73

T=Type of Comment, E = editoral, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
24	NASA	Tice DeYoung	G	Section 4.2, pg. 25	Because each smart card contains the Card Holder Unique Identifier (CHUID) with a Federal Agency Smart Credential Number (FASC-N) and both are accessible without card activation, there is the possibility for tracking of civil servants and contractors without their knowledge or permission. Furthermore, the information on the card may be shared among agencies. What stepps will be taken to avoid unnecessary sharing of data amongh Federal Agencies?	Modify the FIPS-201 language to make it clear that the CHUID and FASC-N will not be used to track civil servants and contractors.
25	NASA	Tice DeYoung	G	Section 4.2, 2nd paragraph, pg. 25	Because both the CHUID and FASC-N records may be read through the contactless interface, how will the data be protected from theft?	Describe the mechanisms to secure the data from theft.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
26	NASA	Tice DeYoung	G	Section 4.2, 4.3 and 4.4 and subsections, pgs. 25-38	Will Systems of Records public notifications be issued for the systems that will store and exchange all the personal and biometeric data on the cards?	Publish the System of Records notifications, if required.
27	NASA	Tice DeYoung	G	Section 4.2.1, pg. 25	The CHUID contains information which uniquely identifies a card. Why add an element associated with the cardholder, the position sensitivity level, in a data element for unique card ID? Especially adding an element that can change, this does not make sense. Changing elements associated with a person are best kept in repository.	Eliminate the position sensitivity level from the mandatory data elements for the CHUID.
28	NASA	Tice DeYoung	G	Section 4.2.2, 3rd paragraph, pg. 26	The section states the certificate shall be a digital signature certificates issued under the X.509 Certificate Policy for the Common Policy Framework [COMMON]. Does this mean the certificate has to be issued by a CA that is part of the Federal PKI Hierarchy? There are a number of existing PKIs in the Federal Government. These should also be acceptable if the agency is cross-certified	Need to re-write this section to reflect the current PKI situation in the Federal Government.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
29	NASA	Tice DeYoung	G	Section 4.3, 2nd & 3rd paragraphs, pg. 27	The 2nd paragraph states the PIV card shall implement key generation. The 3rd paragraph states that key generation is an optional function. Is key generation optional or not?	Need clarification between paragraphs two and three of this section.
30	NASA	Tice DeYoung	G	\Section 4.3, 6th paragraph, 4th bullet pg. 27 and 9th paragraph, 4th bullet pg. 29	One of the optional key pairs listed is the key management key. This could cause some confusion because no mention is made of the encryption or encypherment key pair. The X.509 Certificate Policy for the Common Policy Framework (Common Policy) uses	Provide a definition or description that identifies the terms as equivalent.
31	NASA	Tice DeYoung	T	Section 4.3, 9th paragraph, pg 29	Importing and storing the X.509 certificates for use in PKI path validation violates the FBCA Certificate Policy requirement that the path must be discovered each time before it can be validated	This issue must be resolved in discussions with the FBCA.
32	NASA	Tice DeYoung	G	Section 4.4, 2nd paragraph, pg 30 and Section 4.1.5.1 pg. 23	Section 4.4 states fingerprints shall be the primary biometric utilized in the PIV system so why is electronic facial image a mandatory data element as noted in section 4.1.5.1? Shouldn't it be optional and used by an	Change the requirement for facial image from mandatory to optional and change section 4.1.5.1 and any subsequent sections in which this is mentioned.
33	NASA	Tice DeYoung	G	Section 4.5.3, only paragraph, pg 39	If the PIN pad device activates the PIV card, does this mean that all of the physical access points will have to have both contact and contactless readers at every physical access point? This will be very expensive for	State whether or not both types of readers are required at all physical access points.
34	NASA	Tice DeYoung	G	Section 4.5.3, only paragraph, pg 39	f the PIN pad device activates the PIV card, does this mean that every physical access device must be part of the agencies information technology security solution, that is, behind the firewall(s)? This will be very expensive for agencies to implement.	State whether or not the physical access devices must be inside the agencies IT security perimeter.

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
35	NASA	Tice DeYoung	T	Section 5.1.2, 1st paragraph, pg 40	Will the On-line Certificate Status Protocol (OCSP) responders require signed requests for status? If not, what steps will be taken to reduce the effect of a denial of service attack on the OCSP responders?	Explain the IT security measures being taken to protect the system from denial of service attacks.
36	NASA	Tice DeYoung	G	Section 5.1.2, 1st paragraph, pg 40	Requiring the OCSP responders to respond to every access to a federal building and resource means that the PKI CA Shared Service Providers (SSP) infrastructure will be a costly endeavor. Has NIST done a calculation of what the costs will be? This	Calculate the costs and describe the cost model to be used by the SSP vendors.
37	NASA	Tice DeYoung	G	Section 5.1.2, 1st paragraph, pg 40	Requiring agencies to notify their CA of revoked certificates is already covered by their own CPs and/or with the FBCA CP and/or the Common Policy CP. It does not	Delete these words or change them to say that the agencies must comply with the FBCA CP or the Common Policy CP.
38	NASA	Tice DeYoung	T	Section 5.1.2, 1st and 4th paragraphs, pg 40	The FBCA currently only requires and supports a Certificate Revocation List (CRL). The requirement here for an OCSP responder is inconsistent with this requirement and must be discussed with the	Work with the FPKI-PA to resolve the issue.
39	NASA	Tice DeYoung	T	Section 5.1.2, 4th paragraph, pg 40	Describing the contents of the PKI certificates is covered by the agency CPs, the FBCA CP and/or the Common Policy CPP and doesn't belong in this document.	Delete these words or change them to say that the agencies must comply with the FBCA CP or the Common Policy CP.
40	NASA	Tice DeYoung	T	Section 5.1.2, 4th paragraph, pg 40	What is the relationship between the CA that issues authentication certificates and the agency CA that issues the optional PKI keys? If these aren't the same, this will be costly for agencies to implement	Explain if these two Cas are the same or if they are different Cas.
41	NASA	Tice DeYoun	G	Section 5.2.1.1 pgs. 40-42	This section does not mention capturing the facial image. Where does this take place?	Revise the description in section 5.2.1.1 to include this function.
42	NASA	Tice DeYoung	G	Section 5.2.1.1, 1st paragraph, pg 41	lif a passport is one of the identity documents, this requirement can't be met because it is illegal to copy a passport.	Change the requirement.

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

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
43	Change the require	Tice DeYoung	G	Section 5.2.1.1, 1st paragraph, pg 41	Most (all?) Federal agencies state that making a photocopy of their badge is not permitted. This requirement may not be able	Change the requirement.
44	NASA	Tice DeYoung	G	Section 5.2.2, 1st paragraph pgs. 42-43	This section states the Issuing Authority shall sign the biometrics. Does the Issuing Authority sign using a key issued from a CA that issues certificates to support PIV cards? Or is the Issuing Authority its own CA? Its important to understand this so Agencies know what the full role of the Issuing Authority is.	Please clarify if signing by Issuing Authority is through certificates issued through CA under the Federal Hierarchy or some other CA outside this hierarchy.
45	NASA	Tice DeYoung	G	Section 5.2.2, 2nd paragraph, pg. 43 footnote 3	This footnote states the Issuing Agency is responsible for the necessary PKI certificate management. I do not understand this statement. How is this different than the requirement in section 5.2.3.2 which states agencies can operate CAs/RAs or outsource	Clarify the term, Issuing Agency in footnote three is this a SSP or Agency-operated CA under the Federal PKI Hierarchy?
46	NASA	Tice DeYoung	G	Section 5.2.3.1, only paragraph pg. 43	There is a discrepancy here. If the CA is participating in the hierarchical PKI for the Common Policy, then it cannot have a self-signed, self-issued CA certificate. The root CA for the Common Policy signs the CA certificate of all subordinate CAs, therefore they cannot be self-signed.This footnote states the Issuing Agency is responsible for the necessary PKI certificate management. I do not understand this statement. How is this different than the requirement in section	Rewrite this section.
47	NASA	Tice DeYoung	G	Section 5.2.3.2, 1st paragraph, footnote 4, pg. 43	When will the id-CommonAuth policy be written? It makes compliance impossible until this document is available.	Need to rewrite so that agencies aren't required to comply until some specified time after the poilicy is written.

D = Document,1 = FIPS201, 2 = SP800-73

T=Type of Comment, E = editoral, T = technical

Submitted by: _____

Date: _____

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
48	NASA	Tice DeYoung	G	Section 5.2.3.2.1, 1st paragraph, 1st bullet, pg. 44	If the SIA, AIA and CDP extensions HTTP URIs are optional, why were the SSP vendors required to demonstrate them as part of their Operational Concept Demonstrations? Aren't we in effect making them offer something that no Federal agency	Need to explain the discrepancy.
49	NASA	Tice DeYoung	G	Sections 5.2.4.1 and 5.2.4.2 pg. 46	What role is the "Parent Organization" fulfilling when it verifies the employee is in good standing for renewal and/or re-issue of PIV cards? Is it the RA role, the Approving	Need to clarify who in the prescribed roles needs to verify employee's good standing.
50	NASA	Tice DeYoung	G	Section 5.2.4.3, 2nd paragraph, pg. 47	This section states the Issuing Authority verifies the applicant's new position sensitivity level and completion of ID proofing. To be consistent with previous role descriptions, shouldn't the RA verify the position sensitivity level and send	Revised sentence to state RA responsible for this function not the Issuing Authority.

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