Comment template for draft FIPS 201 and SP 800-73

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	Daon	Denise Mallin	T	2.2 Page 4	Should requires agencies to establish an identity management policy that prevents individuals to take on role substitution, role reversal and multiple roles.	Agencies will develop a normalized set of identity management policies that includes guidelines, methods and processes that prevent individuals to take on multiple roles, role substitutions and/or role reversals.
2	Daon	Denise Mallin	T	2.2 Page 4	Encourage agencies to incorporate technologies, components and systems that document an easily auditable chain-of-custody with regards to the entire PIV process (e.g., application, authorization, registration, issuance and activation). This will be critical for any adjudication and/or prosecution that may or may not need to take place later.	Agencies will evaluate and implement industry best-practices, technology, components and/or systems for both documenting and auditing the PIV chain-of-custody.
3	Daon	Denise Mallin	T	2.2 Page 4	It is not clear what type of organizations qualify for each role in the process. Risk and liability analysis on the part of the federal government should result in, not only a set of roles, but also who or what classification of individuals can fulfill those roles (i.e. contractor, contracting employer, consultant, public trust level x, government employee only, federally regulated entity, outsourced entity, etc.) and this should be a part of this document.	[After a proper risk and liability analysis is completed by a proper governing agency, a table should be created explaining who and what entities are authorized to fulfill a certain role.]
4	Daon	Denise Mallin	T	2.2 Page 4	It is not clear if an individual can possess more than one PIV card. Some special applicants may need more than one PIV. For example, a CIA operative may need to possess more than one PIV.	At no time will any agency issue more than one PIV to a single individual without the express confirmed consent of the PIV Program Managing Agency [Agency X].
5	Daon	Denise Mallin	T	2.2 Page 4	No guidelines are presented concerning how data is viewed, added, deleted or changed by each role at each step in the PIV chain-of-custody. Read only, Write, Append only, rewrite/update, delete, print, send, archive, etc.? Each data element (or group of data elements) should have predefined PIV access and change rules based on each role and the current step in the PIV chain-of-custody. (For example, a Requesting Official should not be able to change a data element once the Authorizing Official has approved the request).	All agencies shall follow the data capture, access, updating, deletion, printing, e-mailing and archival rules outlined in Section 2.2.5 entitled "Data Access and Change Restrictions for the Identity Proofing and Registration Process."

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

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
6	Daon	Denise Mallin	T	2.2.1 Page 5	No standards are cited as to how the information is transported from one role to another (paper only, paper + XML, paper + EFTS, etc.). It is critical as a part of the chain-of-custody that the transport format (not necessarily the transport medium) is clearly defined and adhered to by all agencies.	[A common data structure/format for a PIV envelope should be researched, defined and added to this document. ANSI/NIST ITL 1-2000 and XML are two possibilities that come to mind.]
7	Daon	Denise Mallin	T	2.2.1 Page 5	No standards are cited as to how, when and why notifications are provided from one role to another. It is critical as a part of the chain-of-custody that the notification format, time and format (not necessarily the transport medium) is clearly defined and adhered to by all agencies.	All agencies shall follow the notification rules outlined in Section 2.2.6 entitled "PIV Event and Process Step Notification Rules and Guidelines." [A common notification data structure/format/method for a PIV application event (or step) should be researched, defined and added to this document. E-Mail, XML, EFTS, digital dashboard, website, other portal, etc.]
8	Daon	Denise Mallin	T	2.2.1 Page 5	No standards are cited as to the PIV application/request structure (fields, lengths, digital vs. paper, application number format, etc.)	[A common PIV application form should be developed and attached to this document.]
9	Daon	Denise Mallin	T	2.2.1 Page 5	Are purely digital applications acceptable? Are digital signatures or the use of digital signature pads acceptable? Is the use of another digital biometric acceptable as a signature?	[Minimum and best-practices should be outlined. All digital transactions should be allowed in accordance with federal eGovernment initiatives.]
10	Daon	Denise Mallin	T	2.2.1 Page 5	Simple photocopies of the root identity documents are cited. For more confident comparison functions later in the PIV chain-of-custody and for points of arbitration and any eventual prosecution, color scanned (or photocopied for manual process) documents should be used at a minimum.	The Requesting Official shall submit the PIV request and color scanned 150dpi JPG images (or color photocopied images for manual process) of identity source documents for the Applicant to the PIV Authorizing Official.

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
11	Daon	Denise Mallin	T	2.2.1 Page 6	How does the Registration Authority know that the person appearing in front of them to provide fingerprints is really the applicant whose information appears in the request? Agencies should incorporate additional means by which to assure that the two identities match. This is critical to reduce risk and liability. One option would be snapping a photograph (or even collecting a biometric - say a single fingerprint) at the time the source/claimed identity documents are presented at the first step in the chain-of-custody. Additional low-cost commercial databases and out-of-wallet questions can be leveraged to confirm identity (i.e. Choicepoint - approximately how much is your mortgage each month? A. 750, B 1280, C. 945 or D. 1370?).	Each agency should perform an independent risk and liability assessment to determine what methods of identity confirmation should be required of the Registration Authority in addition to a simple visual check of identity source documents and demographics.
12	Daon	Denise Mallin	T	2.2.1 Page 7	It is not cited how long, what format and at what integrity all of the archived data is to be maintained by the Registration Authority.	The Registration Authority shall be responsible to maintain, for a period of 7 years, until the PIV is renewed/replaced or until the PIV life-cycle ends (whichever occurs first), the following: - Completed and signed PIV request, - … - … - … - Any other materials used to prove the identity of the Applicant.

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
13	Daon	Denise Mallin	T	2.2.1 Page 7	It is not cited if the Registration Authority can maintain a record of the applicant's fingerprint record for the purposes of 1) adjudication, 2) prosecution or 3) resubmission to comply with specific job position requirements (i.e. some positions require a yearly criminal history check be completed).	The Registration Authority may maintain a copy of the fingerprint data (in compliance with the US Privacy Act) for a period of up to five years ONLY after the Registration Authority has passed a technical and privacy policy and system review by the PIV Program Managing Agency [Agency X]. The copy of the fingerprint data can ONLY be used for the purposes of: 1) adjudication, 2) prosecution or 3) resubmission to comply with specific job position requirements (i.e. some positions require a yearly criminal history check be completed) .
14	Daon	Denise Mallin	T	2.2.2 Page 7	It is not cited what triggers an automatic renewal (time limit reached, address changed, etc.), revocation (job duty change) or flagging (certain events have occurred or have been attempted) of a PIV.	Each agency should perform an independent risk and liability assessment to determine what event triggers are used to determine if a PIV needs to be renewed, revoked or flagged, beyond what is already outlined in Section 2.2.7 entitled "Mandatory PIV System and Process Actions Required as a Result of Specific Events."

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

Submitted by: ______________________________________

Date: _______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
15	Daon	Denise Mallin	T	2.2.3 and 2.3 Page 7	It is not cited what information access rights, and adjudication rights, an applicant has if his PIV is still pending or has been denied.	Each agency should perform an independent risk and liability assessment to determine what logical and physical access controls are implemented for an individual while his or her PIV application status is pending. If the individual is denied a PIV and/or employment, the PIV applicant will be granted access to relevant information and an adjudication process in accordance with the US Freedom of Information Act and guidelines outlined in section 2.3.1 entitled "PIV Applicant Adjudication Process and Guidelines."
16	Daon	Denise Mallin	T	2.3 Page 7	How does the Issuing Authority know that the person appearing in front of them to pickup and activate the PIV card is really the applicant whose information appears in the request and whose fingerprints were captured at registration? Agencies should incorporate additional means by which to assure that the two identities match. This is critical to reduce risk and liability. One option would be snapping a photograph (or even collecting a biometric - say a single fingerprint) at the time the source/claimed identity documents are presented at the first step in the chain-of-custody. Additional low-cost commercial databases and out-of-wallet questions can be leveraged to confirm identity (i.e. Choicepoint - approximately how much is your mortgage each month? A. 750, B 1280, C. 945 or D. 1370?).	Each agency should perform an independent risk and liability assessment to determine what methods of identity confirmation should be required of the Issuing Authority in addition to a simple visual check of identity source documents and demographics.
17	Daon	Denise Mallin	T	2.3 Page 7	The Issuing Authority needs to somehow notify the Requesting and Authorizing Authority as to the status of the PIV issuance. Has the card been picked up and activated? When? Proof?	The Issuing Agency will notify, with reasonable supporting documentation, that the proper individual has picked-up and activated his or her PIV card, in accordance with the notification rules outlined in Section 2.2.6 entitled "PIV Event and Process Step Notification Rules and Guidelines.".

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

Submitted by: ______________________________

Date: ____________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
18	Daon	Denise Mallin	T	2.3 Page 7	It is not cited how long, what format and at what integrity all of the archived data is to be maintained by the Issuing Authority.	The Issuing Authority shall be responsible to maintain, for a period of 7 years, until the PIV is renewed/replaced or until the PIV life-cycle ends (whichever occurs first), the following: - Completed and signed PIV request, - … - … - … - Any other materials used to prove the identity of the Applicant.