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	G	Page 11 - 3.2.1	PIV Project Managing Agency should incorporate policies, methods and processes that include ways to detect PIV system negligence and non-conformity.	All agencies will include mechanisms, methods and/or processes in their PIV policies and guidelines to detect PIV system negligence and non-conformity.
2	Daon	Denise Mallin	T	Page 11 - 3.2.2	Additional responsibilities of the PIV applicant / cardholder.	Applicants/cardholders are responsible for: - Reporting any loss, theft or known PIV system breach immediately, once issued their PIV. - Following all published rules, guidelines and best-practices for handling PIV cards to prevent theft and loss.
3	Daon	Denise Mallin	T	Page 12 - 3.3	The PIV Card Issuance and Management Subsystem also should include overall identity management functions, not just card management. We suggest adding 'Identity' to the title.	***PIV Card Issuance and Identity Management Subsystem*** **-** the components responsible for identity proofing and registration, card issuance and key management, as well as the various repositories and services (PKI credentials, certificate status servers, etc) required as part of the verification infrastructure.
4	Daon	Denise Mallin	T	Page 13 - Figure 3-1	Show the (optional) ability for Physical Access Control to communicate with the PKI Directory/Certificate Status Responder	Draw a line with right arrow between PKI Directory graphic and Physical Access Control graphic/box.
5	Daon	Denise Mallin	T	Page 14 - 3.3.1	Some agencies may wish to provide cardless access to certain resources (i.e. biometric only, biometric + PIN, etc.) to protect an individual's anonymity within a given population (a good example is an undercover LEO), to deal with lost or forgotten PIV cards, or for logical access to a computer. Is this a provision of PIV? Agencies may also wish to verify the biometric against a centrally maintained reference database, versus against the biometric stored on the card.	[Make clear how cardless access and/or matching to centralized reference data can be used as an option available to an agency when designing their PIV system. This is especially critical when dealing with lost or forgotten PIV cards.]
6	Daon	Denise Mallin	E	Page 14 - 3.3.2	Revise Section Title (See earlier comment)	**PIV Card Issuance and Identity Management Subsystem**

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
7	Daon	Denise Mallin	T	Page 14 - 3.3.2	Section indicates that certain data is stored in the Registration Repository but does not outline which data, how it should be stored and for how long. Please see Daon PIV Comment Sheet - Part I.xls, Items 12, 13, 17, and 18.	Please see Daon PIV Comment Sheet - Part I.xls, Items 12, 13, 17, and 18.
8	Daon	Denise Mallin	E	Page 15 - 3.3.3	"Physical and logical resources are the end targets of the entire PIV system." is unclear. Consider rewording.	Authentication used to control access to physical and logical resources is the end goal of the PIV system.
9	Daon	Denise Mallin	E	Page 15 - 3.3.3	"…Identification & Authentication (I&A) component…" *Identification* is the function by which a person's identity is determined without any presented claim of identity. *Verification* is the function by which a person's claimed identity is verified by comparing one or more claimed identity attributes with each corresponding identity attribute already enrolled. *Validation* is the function by which a person's identity attribute (and/or claimed identity attribute) is confirmed as valid (usable/allowed) by a recognized/authorized governing agency or system (whether already enrolled or not). *Authentication* is a function by which a person's identity attribute (and/or claimed identity attribute) is confirmed (or declared) to be authentic (not a counterfeit) by a recognized/authorized governing agency or system (whether already enrolled or not). An identity attribute can be declared valid (validated) without properly being checked for authenticity (authenticated). A claimed identity attribute can be verified by the system without that attribute ever being validated or authenticated.	The PIV Access Control Subsystem could conduct all of these functions depending on the business rules defined by the particular agency. Ideally, the PIV Identity Management System should control all validations and authentications while the PIV Access Control Subsystem can conduct identifications and verifications. In addition, however, a validated list could be copied to the PIV Access Control Subsystem and then kept up to date.
10	Daon	Denise Mallin	E	Page 16 - 3.4	It should be noted that special precautions should be taken during the PIV Card Maintenance activity to prevent unauthorized or rogue applications and data from being introduced to the card.	"…and biometrics stored on it. It should be noted that this activity must follow specific policies and procedures reflected in the technical implementation to minimize susceptibility to unauthorized applications or data."

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
11	Daon	Denise Mallin	T	Page 21 - 4.1.4.2.a.	Agency Serial Number - Although the numbers may be the same across agencies, the format should be standardized to prevent confusion when the card is used at 3rd party agencies.	[Specify a format that all agencies should use.]
12	Daon	Denise Mallin	T	Page 21 - 4.1.4.3.a.	Signature - The space for the signature appears so small that it may be useless for any kind of manual examination. It appears to serve no other purpose. Enlarge or remove.	Enlarge area for signature or remove completely.
13	Daon	Denise Mallin	T	Page 23 - 4.1.5.1	Why is "match-on-card" the only method for CTC authentication with biometrics? Why not embedded matching in the card reader that meets or exceeds some designated security model (i.e. FIPS level)?	"Biometric information may optionally be used in CTC authentication if the PIV card implements on-card or in-device matching of the biometric information."
14	Daon	Denise Mallin	T	Page 24 - 4.1.6	Why is "match-on-card" the only method for activating the card other than a PIN? There are only very few biometric providers that have spent the R&D and production dollars required for match-on-card. By limiting this at card activation, it quickly implies which vendors may also be the first to be used for all other forms of authentication (i.e. CTE) when the card is used.	[Consider allowing CTE biometric or a sophisticated centralized method of card activation, keeping strict requirements in mind to prevent unauthorized activation.]
15	Daon	Denise Mallin	T	Page 25 - 4.2.1	Why does the CHUID contain the position sensitivity level, other than for access speed? There are instances where individuals will need to maintain anonymity with respects to their access level or capabilities. Plus, a simple interrogation of the card will result in knowing the access level for that card...this could be very dangerous and is risky.	[Consider an alternate way to know the security access level written to a specific card other than simple interrogation of the CHUID.
16	Daon	Denise Mallin	T	Page 30 - 4.4	It is quite limiting to prevent the transfer of biometric information through the contactless interface. Keep in mind ICAO has approved this already for passports. Other intelligent ways to protect the biometric information and prevent unauthorized biometric access could easily be designed. Read/write access will also be limited due to this choice.	[Consider other advanced ways available to protect biometric information to enable the use of applications that would benefit greatly from the use of the contactless interface.]

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
17	Daon	Denise Mallin	T	Page 30 - 4.4.1	Daon is concerned with the plan to use only four-finger and thumb slap impressions for the purposes of criminal and/or terrorist background checks. Matching accuracies are significantly reduced when using plain impression finger images due to inconsistent and reduced surface areas. High quality rolled or rolled-equivalent images should be required for all background checks. If the PIV requirements compromise on this, PIV could endanger our National security. For example, consider that all public trust positions already rely on ***rolled*** 10-prints for history checks; the PIV requirements would actually reduce the integrity of the checks already being performed today. Also note that the use of high-quality rolled or rolled-equivalent images would result in better matching rates when the card is authenticated (CTC or CTE) with a higher tolerance for finger rotation when the live plain image is captured.	"The biometric data supplied for biometric identification search shall consist of a complete set of ten rolled (or rolled-equivalent) impressions obtained from all fingers with full sequence assurance. Plain impressions (also called slap or flat) will also be collected only if required for sequence assurance."
18	Daon	Denise Mallin	T	Page 31 - 4.4.3	Daon is concerned with the plan to use only four-finger and thumb slap impressions for the purposes of criminal and/or terrorist background checks. Matching accuracies are significantly reduced when using plain impression finger images due to inconsistent and reduced surface areas. High quality rolled or rolled-equivalent images should be required for all background checks. If the PIV requirements compromise on this, PIV could endanger our National security. For example, consider that all public trust positions already rely on ***rolled*** 10-prints for history checks; the PIV requirements would actually reduce the integrity of the checks already being performed today. Also note that the use of high-quality rolled or rolled-equivalent images would result in better matching rates when the card is authenticated (CTC or CTE) with a higher tolerance for finger rotation when the live plain image is captured.	"The captured images will shall be rolled (or rolled-equivalent) impressions obtained from all fingers with full sequence assurance. Plain impressions (also called slap or flat) will also be collected only if required for sequence assurance."

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
19	Daon	Denise Mallin	T	Page 32 - 4.4.3	Daon is concerned with the plan to use only four-finger and thumb slap impressions for the purposes of criminal and/or terrorist background checks. Matching accuracies are significantly reduced when using plain impression finger images due to inconsistent and reduced surface areas. High quality rolled or rolled-equivalent images should be required for all background checks. If the PIV requirements compromise on this, PIV could endanger our National security. For example, consider that all public trust positions already rely on ***rolled*** 10-prints for history checks; the PIV requirements would actually reduce the integrity of the checks already being performed today. Also note that the use of high-quality rolled or rolled-equivalent images would result in better matching rates when the card is authenticated (CTC or CTE) with a higher tolerance for finger rotation when the live plain image is captured.	[Replace image size, capture steps and ANSI record type to reflect the use of ROLLED or ROLLED-EQUIVALENT finger images to ensure the highest level of matching accuracy and National security.]
20	Daon	Denise Mallin	T	Page 33 - 4.4.3	Daon is concerned with the plan to use only four-finger and thumb slap impressions for the purposes of criminal and/or terrorist background checks. Matching accuracies are significantly reduced when using plain impression finger images due to inconsistent and reduced surface areas. High quality rolled or rolled-equivalent images should be required for all background checks. If the PIV requirements compromise on this, PIV could endanger our National security. For example, consider that all public trust positions already rely on ***rolled*** 10-prints for history checks; the PIV requirements would actually reduce the integrity of the checks already being performed today. Also note that the use of high-quality rolled or rolled-equivalent images would result in better matching rates when the card is authenticated (CTC or CTE) with a higher tolerance for finger rotation when the live plain image is captured.	[Replace the table with the field list for all ten rolled or rolled-equivalent records.]

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
21	Daon	Denise Mallin	T	Page 34 - 4.4.4	No accommodations for alternate fingers are listed in case the fingers or hand are missing or unusable.	"If the left or right index fingers are not usable or are missing, alternate fingers may be designated for capture using the following priority table that follows." [Insert Alternate Finger/Hand Priority Table].
22	Daon	Denise Mallin	T	Page 37 - 4.4.5.8	Facial Image Quality - Highly subjective in nature and nearly impossible to implement in a consistent way. May be better to wait until NIST defines more objective image quality measurements.	
23	Daon	Denise Mallin	G	Page 39 - 4.5.2	Some of the leading smart card reader/writer manufacturers do not conform to PCSC standards due to their legacy in the financial sector. This significantly limits the number of potential card reader/writer vendors.	
24	Daon	Denise Mallin	T	Page 47 - 5.2.4.3	PIV Update - How about if the position sensitivity is reduced? Can the card be simply updated rather than replaced?	[Provide guidance on when the position sensitivity is reduced].

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