Submitted by: _____Carolyn Merek, US Department of Justice_____

Date: _____12/22/04_____

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	DOJ/CJIS	Brian D. Finegold	G	PIV-II, 4.4.5	The Standard indicates the facial image type is defined by ANSI/INCITS 385-2004. It's not clear whether this is compatible with ANSI/NIST ITL-2000 Type-10 mugshot record, and taken using ANSI/NIST best practices for mugshot.	
2	DOJ/CJIS	Brian D. Finegold	T	4.1.6.1	This paragraph says "every pin card shall implement PIN-based cardholder activation". It then goes on to say "may optionally implement activation using biometric information stored on the card". It is not clear if the biometric implementaiton is an addition to a mandatory PIN implementation or allowed as an alternative.	
3	DOJ/CJIS	Brian D. Finegold	T	4.1.6.1 and 6.1.3	Paragraph 4.1.6.1 says "The biometric information shall be transmitted to the PIV card, and using biometric match-on-card, compared with the stored biometric info (e.g., image or template). However, paragraph 6.1.3 says "The signed biometric may be used to support an authentication mechanism through a match-off-card scheme.,,, Is it match-on-card or off-card, image, or template?	
4	DOJ/CJIS	Brian D. Finegold	T	4.4.1	In para 4.4.1, it says" biometric data supplied for biometric identification search shall consist of a complete set of ten "slap" fingerprints which may alternatively accompanied by a set of ten rolled fingerprint images (emphasis added)." It is not clear why the rolled prints are necessary, and just confuses the implementation methodology.	
5	DOJ/CJIS	Brian D. Finegold	T	4.1.4.2b and Page 20	This specifies that a five-digit number that uniquely identifies the issuing facility within the agency, but the example on page 20 only has 4 digits? Which is correct?	

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

Submitted by: _____Carolyn Merek, US Department of Justice_____

Date: _____12/22/04_____

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	DOJ/CJIS	Brian D. Finegold	G	PIV-I	The standard lays out a schema that defines the roles and responsibilities of authorities from requesting official to authorizing official to Registration Authority to Issuing Authority, and says the Registration authority is to capture the ten fingerprints for the background check. After completion of the background check, the Registration Authority shall notify the Issuing Authority than an identity credential can be issued. Not addressed is how the fingerprint information is to be forwarded from the Registration Authority to the Issuing Authority so it can be included on the PIV card.	
7	DOJ/CJIS	Brian D. Finegold	E	PIV-II	It it not certain that with as many uncertainties as exist in this standard, that any agency will be able to complete a procurement of cards and readers in the timeframe specified. There are many implementation decisions which seem to be left up to each individual agency which will take time to resolve. Additionally, it is unknown how long it will take NIST to certify the card issuers.	
8	DOJ/Security and Emergency Planning Staff	J. Massillon	T	Page 22. Section 4.1.4.3.e zone	Agency Name & Department should be optional because if the ID is lost or stolen, an outside source could attempt to use the badge to obtain access to the agency. It should not be required to include any DOJ agency identifier.	
9	DOJ/Security and Emergency Planning Staff	J. Massillon	G	Page 6, 2nd para. And, page 7 section 2.2.3	It will take too long to wait for a background investigation to be complete to issue the permanent credential. An employee/contractor may not be able to access space needed to perform work because they would only have a visitor credential.	There needs to be an interim process in place to ensure employee can be productive from the time they come on board until the background check is complete (e.g., Temporary credential issued based on a clear name and fingerprint check).

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

Submitted by: _____Carolyn Merek, US Department of Justice_____

Date: _____12/22/04_____

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
10	DOJ/ATF	Mitchell Arnone	T	PIV-I, 2.3	Part I paragraph 2.3 states that a picture will be taken at the time of credential issuance and a copy retained. Should there be specific guidance on how to store those images (e.g. in a separate repository or in the agency directory)? There must be a reason for retaining the image and the method of archive must be in support of this reasoning. Furthermore, it is assumed that this image must be maintained in electronic form and therefore capable of being accessed remotely. Should these images be available for access by other agencies that rely in the credential for the purpose of physical access? If so, will there be a single system developed for this purpose? Does this raise issues regarding privacy information?	
11	DOJ/ATF	Mitchell Arnone	G	4.1.3.g	Should a standard card holder/container specification be defined since the card will not be allowed to have a hole punched in it? (very minor technicality)	
12	DOJ/ATF	Mitchell Arnone	E	PIV-II	The ATF has deployed a proximity card from HID that uses 125 kHz RFID to communicate with contactless card readers for physical access. This technology is currently in use at most (if not all) ATF locations and it is also being planned for in the new ATF headquarters. Any change to this will require significant investment to upgrade existing infrastructure. The ATF will need to understand as soon as possible whether or not a waiver will be considered allowing us to deviate from this standard and the conditions on which the waiver may be granted.	

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

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

Submitted by: _____Carolyn Merek, US Department of Justice_____

Date: _____12/22/04_____

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	DOJ/ATF	Mitchell Arnone	E	PIV-II	Adoption of a smart card that can support both the HID (125kHz) and the ISO 14443 13.56Mhz (MIFARE) contactless chips/antennas would be highly recommended in order for the ATF to be able to deploy a single card that can support both technologies. By deploying a card body that supports both the HID proprietary and MIFARE, the ATF can migrate away from HID over time without having to reissue new smart cards and with little or no impact on the end user.	
14	DOJ/ATF	Mitchell Arnone	T	4.4	Paragraph 4.4 states that "The biometric data on the PIV card may only be read from an activated card through the contact interface". If this is the case, then biometrics can not be used for physical access unless a contact based access control system has been deployed (which is very uncommon). For physical access, it is common practice to store biometrics on the MIFARE (contactless) chip or on some type of back end system. Reading further in paragraph 6.1.3, it seems to indicate that biometrics can be used for physical access, which would then infer that biometrics are being stored on the MIFARE chip and will be accessed through a means other than the contact chips. It is highly recommended that the accepted methods of using biometrics be explicitly defined in a consistent manner throughout the PIV standard.	
15	DOJ/ATF	Mitchell Arnone	G	PIV-II, Section 6	Section 6 needs to define better when match-on-card and match-off-card are permitted. In my experience, match-on-card is required for logical access while match-off-card is used for physical access (match-off-card is possible for logical access but not desirable). Back-end systems for physical and logical access typically do not communicate.	
16	DOJ/ATF	Mitchell Arnone	T	4.1.2	When embedding of the OVD or OVI, can it be covered with a transparency or lamination?	

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

Submitted by: _____Carolyn Merek, US Department of Justice_____

Date: _____12/22/04_____

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	DOJ/ATF	Mitchell Arnone	T	4.1.5.1	Paragraph 4.1.5.1 seems to indicate that encryption/decryption key pairs will not be allowed on the PIV card. The storage of asymmetric keys, used for the purpose of encryption and decryption, should be explicitly addressed.	
18	DOJ/ATF	Mitchell Arnone	T	5.1.2	Paragraph 5.1.2 states that "every CA that issues PIV authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues." Should there be additional guidance on which systems will be expected to use PKI credentials for purposes such as authentication, digital signatures and data confidentiality (encryption)? For example, Active Directory can be easily enabled for smart card/PKI authentication. Will this become mandatory or optional? Most Agency internal applications will require some degree of modification to become PKI enabled. Will this too become mandatory or optional? Any guidance would be greatly appreciated.	
19	DOJ/Security and Emergency Planning Staff	J. Massillon	G	4.1.4	Identity card characteristics should visually differentiate employees from contractors	
20	DOJ	C. Merek	G	4.1.4	Identity card non-mandatory elements should be standardized to the degree practical and should be discouraged from performing critical acess control function for a government controlled facility or federally controlled information system.	

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