Submitted by: William D. Schroer
President, Optikey, LLC
702-336-2858
wds@optikeysecurity.com
Date: 23 December 2004

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	Optikey, LLC	William Schroer 702-336-2858	General	FIPS Pub 201, Section 2.1, Page 4	Bullet #5 doesn't provide remote or on-the-spot verification of an employee or contractor.	to read…..that supports rapid electronic authentication of Federal employees and contractors with, or without access to a central data bank or system
2	Optikey, LLC	William Schroer 702-336-2858	General	FIPS Pub 201, Section 2.1, Page 4	Bullet #4 calls for identity credentials that are resistant to fraud, tampering, etc. Paragraph 2.1 should also list identity credentials that are impossible to successfully duplicate as a desireable feature.	It is desireable for an identity card to be impossible to successfully duplicate, copy, or counterfeit.
3	Optikey, LLC	William Schroer 702-336-2858	General	FIPS Pub 201, Section 3.1, Page 10	Mitigation of threats should also stipulate that a PIV card is valid with or without the use of linkage to a central data system.	Provide a PIV card that may subsequently be ussed to verify the cardholder (an Applicant who is issued a PIV card) identity, and authenticity of the card, rapidly and securely with or without the use of a central data bank.
4	Optikey, LLC	William Schroer 702-336-2858	General	FIPS Pub 201, Section 3.1, Page 11	Protection against counterfeit or cloned cards should include on-the-spot or remote verification and authentication of the card	Provide protection against use of cloned or counterfeited PIV cards with or without the use of a central data bank.

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

Submitted by: William D. Schroer
President, Optikey, LLC
702-336-2858
wds@optikeysecurity.com
Date: 23 December 2004

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
5	Optikey, LLC	William Schroer 702-336-2858	Technical	FIPS Pub 201, Section 4.1.2a, Page 17	NIST has developed Optical Maximum Entropy Verification (OMEV) technology with secure, unique anti-counterfeiting keys. This technology has been proven by NIST to be unbreakable, low cost, and virtually impossible to detect with the human eye. Ref: NIST-OMEV Contract #: 70NANB7H3010	In addition to OVD or OVI technologies Optical Maximum Entropy Verification (OMEV) technology with secure, unique anti-counterfeiting keys shall be incorporated to prevent fraudulent reproduction.
6	Optikey, LLC	William Schroer 702-336-2858	Technical	FIPS Pub 201, Section 4.4, Page 30	Biometric information should be protected through a validation process that first identifes the card as authentic and then, and only then, should the biometric information be validated/approved. Biometric information such as fingerprints should be verifiable with or without access to computer networks.	One-to-one fingerprint matching shall be performed for PIV identity verification with or without the use of network access to computer data banks. Verification of fingerprint biometric information shall only be accomplished after the authentication of the PIV card has been established. This linkage between an authentic PIV card and on-the-scene biometric verification is necessary.

Comment template for draft FIPS 201 and SP 800-73

Submitted by: William D. Schroer
President, Optikey, LLC
702-336-2858
wds@optikeysecurity.com
Date: 23 December 2004

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	Optikey, LLC	William Schroer 702-336-2858	Technical	FIPS Pub 201, Section 4.4, Page 30	Biometric information is typically stored in electronic media and/or visibly present on the PIV. As an added measure of security, it is proposed that fingerprint/thumbprint data be embedded with Optical Maximum Entropy Verification (OMEV) analog structures as a binary coding that is invisible to the human eye. The processing of this data can be accomplished during the PIV issuance This will provide unbreakable verification of the fingerprint or thumbprint of an individual vs. the digital or visual information on the card.	Biomatric data shall be incorporated in the PIV through conventional methods. Additionally, fingerprint or thumbprint information shall be embedded and linked with Optical Maximum Entropy Verification (OMEV) technology to provide an added level of security. Verification of fingerprint or thumbprint data shall be accomplished with or without the use of a central data bank.
8	Optikey, LLC	William Schroer 702-336-2858	Technical	FIPS Pub 201, Section 6.1.3, Page 52	Protection against counterfeit or cloned biometric data should include on-the-spot or remote verification and authentication of the card	10) Cardholder biometric authentication shall be accomplished with, or without the use of a central data bank.

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

Comment template for draft FIPS 201 and SP 800-73

Submitted by: William D. Schroer
President, Optikey, LLC
702-336-2858
wds@optikeysecurity.com
Date: 23 December 2004

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
9	Optikey, LLC	William Schroer 702-336-2858	General	FIPS Pub 201, Section 3.3, Page 12	Security agencies and organizations should have the flexibility to conduct on-the-spot authtications of PIV cardholders. A handheld reader that has the ability to authenticate the PIV card and secondly authenticate the PIV cardholder biometric information	PIV System Front-End Subsystem. …..logical access to the desired Federal resource. Security agencies and organizations must have the ability to conduct on-the-spot authentications with a handheld reader that is capable of authenticating the PIV card and the cardholder biometric information.

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