Subject: Comments on Public Draft FIPS 201
From: "Bone, Joseph (Mike) CIV NAVSURFWARCENDIV Crane, Code 4041" <joseph.m.bone@navy.mil>
To: <DraftFips201@nist.gov>

See attached comments.

Mike Bone
Crane Division, Naval Surface Warfare Center (NSWC Crane)
Harnessing the Power of Technology for the Warfighter
Code 4041, Bldg. 39
300 Hwy 361
Crane, IN 47522-5001
Ph: 812.854.1141
Fax: 812.854.1340
Email: joseph.m.bone@navy.mil

 MikeBoneComments.xls

Submitted by: Mike Bone, NSWC Crane
Date: December 22, 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	NSWC Crane	Mike Bone	G	4.3, pp. 27	Currently, the DoD CAC card has an asymmetric key pair for encryption of e-mail and other documents. The list of mandatory and optional keys in this section does not include an encryption key pair.	Ensure that DoD no longer has a requirement for an encryption key pair. If they do require it, add it to the list of mandatory or optional keys, addressing escrow issues. Alternatively, if one of the keys currently defined in the draft FIPS 201 are to be used for encryption, please clarify this.
2	NSWC Crane	Mike Bone	E	4.5.1, pp. 38	PC/SC is specified for all contact readers. PC/SC is intended for interface between reader and host system, but some contact readers intended for physical access do not connect to a host PC.	Change wording of this section to indicate that only contact readers that interface with a host PC are required to support PC/SC, as in section 4.5.2 for contactless readers.
3	NSWC Crane	Mike Bone	T	Table 6-1, pp. 55	For the PACS medium assurance profile, the comments state that no change is required to PIV card for access to a new facility. This seems to contradict section 6.1.2, pp. 51, last item in 2nd numbered list, that mentions use of a site-specific key to compute the HMAC. If a site-specific key is used to create and verify an HMAC, the PIV will require a change for a new site.	Please clarify this discrepency. This may also indicate a problem in the V2.2 PACS Guidance. In section 3.3 of that document, a site-specific key is mentioned in the description of the high assurance profile verification process. Step 8 states that the result of the computations up to that point is the HMAC used for the medium assurance profile. But there is no mention of how multiple HMACs computed using different site-specific keys are to be supported for the medium assurance profile.

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