"Comment template for draft FIPS 201 and SP 800-73
Submitted by: Jonathan L. Hale Jon Hale Associates, Inc. (630) 420-8837

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
1	Jon Hale & Associates, Inc.	Jonathan Hale	G	Section 6.2.1	I disagree with the concept that physical access points are typically not connected to an agency's logical network or the Internet. Although most access control systems make decisions locally through a distributed processing panel, they are typically linked to a central server or host processor and do communicate "on-line".
2	Jon Hale & Associates, Inc.	Jonathan Hale	G	Section 4.4	The current specification appears to allow only the inclusion of a fingerprint and facial recognition biometric on the card. These are only avaiulable for use through the contact smart card technology under the "assumption" that privacy and security concerns can not be met with the RF smart card technology.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, 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)
				Section 6.1.3	The specification requires entry of the stored PIN in order to read the biometric template. The reader can read the CHUID as a PIN without requiring the entrant to perform a separate step. This actually requires the entrant to submit three forms of identification, token, PIN, and biometric. In many cases, only two are required.

Proposed change
Local security directors of agencies are unwilling to accept clearance for personnel who are "unknown" to them and generally permit only limited access to select portals. Once outsiders have been personally vetted by local management, permissions are added to the system to grant more extensive physical access. The central Government Certificate Authority" will have to be a central server data base of all cardholders, and include the issuing agency. A data link will need to be established between each agency master Certificate Server to post changes (adds, deletes) to the central Government server.
The specification should allow the addition of other biometric templates such as hand geometry, and iris scan to the card as options. The cards should allow access to all biometric technologies through the RF smart card. Current encryption technologies provide sufficient security to allay concerns over security and confidentiality of data. The market currently includes RF smart card readers connected to a biometric reader. When the card is presented, the template is loaded into the biometric reader and the entrant is asked to present himself for verification. It does not appear that the current specification will allow this technology to remain in use. Agencies with these technologies will have to remove them or carry two cards if the specifications are left unchanged.

"Comment template for draft FIPS 201 and SP 800-73
Submitted by: Jonathan L. Hale Jon Hale Associates, Inc. (630) 420-8837

Proposed change
Use of the biometric template should be made available simply by having a smart card reader associated with a biometric reader. When the smart card is read, the CHUID forms the initial PIN entry, the template is downloaded to the biometric device, and the entrant is prompted to proceed with the biometric procedure.

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