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)
1	R223	scluthe	T	1.1 page 9	SP800-73 specifies an obsolete version of GlobalPlatform Version 2.0.1
2	R223	scluthe	E	2.2 page 11	Acronym PIV is given twice with different meaning
3	R223	scluthe	E	2.3 page 12	inconsistent use of capital letters in "Mandatory (M), optional (O) or conditional (C)."
4	R223	scluthe	E	3.0 page 13	extra word "is" in last sentence of the section: "program interface is may be different"
5	R223	scluthe	T	3.2.2 page 16	This section introduces the concept of an "organization-specific card application" but could go further and introduce the concept of organization-specific application domains whereby GlobalPlatform Security Domains are are utilized to create separate areas on the card for groupings of organization-specific applications and data.
6	R223	scluthe	T	3.2.4 page 16	"At most one card application shall be active on the PIV integrated circuit card at any time." seems to indicate that logical channels as defined in ISO 7816-4 are not supported.
7	R223	scluthe	T	3.2.7 page 17	Figure 1 & associated discussion leave out the possibility that an application F might utilize a sharable interface (in the JavaCard sense) provided by application E. These applications might interact but not through their respectve data repositories as shown with Applications A & B.
8	R223	scluthe	E	3.3 page 17	"The individuals mentioned in an access control must be authenticated by the card before the operations by the rule are allowed." doesn't make sense.
9	R223	scluthe	E	3.4.1 page 19	spelling error: connetion

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, 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)
10	R223	scluthe	T	3.4.1 page 19	"The other method secures a single card command. This method called secure messaging and is used with card commands other than card commands for content management." is a misrepresentation of the capabilities of the ISO-7816-4 feature. Specifically the cryptographic checksum capability calls out that the chaning block comes from the final check block of the previous command or reponse. Also, the reason secure channels are only good for content management is that there is no security in existing secure channel protocols for the response APDUs.
11	R223	scluthe	E	3.6 page 20	"Chapter xxx of this FIPS." is incomplete and also this is not a FIPS, it is a special publication
12	R223	scluthe	E	4.2 page 22	Algorithm identifiers are not specified.
	R223	scluthe	T	4.2 page 22	Insufficient algorithms/key sizes are specified
13	R223	scluthe	E	4.4 page 23	Meaning of M/O not specified in Table 4.2
14	R223	scluthe	E	4.5 page 23	Meaning of M/O not specified in Table 4.3
15	R223	scluthe	E	4.8 page 23	Meaning of M/O not specified in Table 4.4
16	R223	scluthe	E	4.11 page 24	Meaning of M/O not specified in Table 4.5, 4.6, 4.7
17	R223	scluthe	T	5.2 page 33	The API for application management doesn't appear to support the concept of "orgaization specific application domains" see comment #5 above.
18	R223	scluthe	T	6 page 51	Table 6.1 allows for the security of all commands except for DELETE FILE. This deficiency could be used to create a denial of service through a man-in-the-middle attack by removing valuable data from the card.
19	R223	scluthe	T	6.2.1 page 59	Table 6.9 needs to include EC-256 & EC-384 for National Security Systems

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, 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)
20	R223	scluthe	E	6.2.1 page 59	Extra fields in Table 6.9 should be changed to RFU
21	R223	scluthe	E	6.2.1 page 59	Extra fields in Table 6.10 should be changed to RFU
22	R223	scluthe	E	6.2.1 page 59	It is unclear if Table 6.9 correlates to tag '81'
23	R223	scluthe	E	6.5 page 78	Meaning of M/O not specified in Table 6.14
23	R223	scluthe	E	6.5.1 page 78	Meaning of M/O not specified in Table 6.15
23	R223	scluthe	E	6.5.1 page 78	Meaning of M/O not specified in Table 6.16
23	R223	scluthe	E	6.5.2 page 79	Meaning of M/O not specified in Table 6.17
23	R223	scluthe	E	6.5.2 page 79	Meaning of M/O not specified in Table 6.18
23	R223	scluthe	E	6.5.3 page 79	Meaning of M/O not specified in Table 6.19
23	R223	scluthe	E	6.5.3 page 80	Meaning of M/O not specified in Table 6.20

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

Submitted by: _____

Date: _____

Proposed change
specify current GlobalPlatform 2.1.1
change first PIV (Integrated Circuit Card for Identification) to PIV-ICC
change to all capital or all lowercase letters.
remove word "is"
introduce security domains to contain organization-specific versions of the card applications for interoperable use.
Clarify if logical channels are supported.
Clarify if inter-application communication is supported, optional, or prohibited.
rewrite as: "The individual mentioned in an access control rule must be authenticated by the card before the operation is allowed."
change to connection

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

Submitted by: _____

Date: _____

Proposed change
Change to specify that secure messaging can be used to secure a sequence of commands and responses as well as a single command/response pair.
rewrite.
Additional algorithms should be specified to support National Security Systems: AES-128, AES-192, AES-256, ECC 256, ECC 384.
include legend
include legend
include legend
include legends
Add capability to add an application under another application (security domain).
Add secure messaging to DELETE FILE.
Add EC-256 & EC-384 fields for National Security Systems

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

Submitted by: _____

Date: _____

Proposed change
Change unspecified rows to RFU
Change unspecified rows to RFU
clarify relationship of Table 6.9 to tags
include legend
include legend
include legend
include legend
include legend
include legend
include legend

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