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	RU Consulting	Rick Uhrig	G	Not Present	**Graduated Criteria.** Graduated criteria could and should be specified for each of the four named objectives in HSPD-12: (a) Identity proofing (b) Resistance to fraud & tampering (c) Electronic authentication (d) Issuance & accreditation\
2	RU Consulting	Rick Uhrig	G	Not Present	**Issuer Accreditation Requirements.** HSPD-12 requires that issuer reliability be established through an official accreditation process. No accreditation requirements are included in 201 PUBLIC Draft

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)
3	RU Consulting	Rick Uhrig	G	D1 Throughout	**Allowance for Dedicated Digital Signing PIN.** FIPS 201 PUBLIC Draft as written appears to assume that the card has a single PIN, and that this PIN activates both the card and the digital signature. Having a single PIN for all PIV functions is a major vulnerability in the PIV system. To close this vulnerability, digital signing must be separated for all other functions. In a perfect world there would be physical separation (i.e. enabled on an entirely different chip card). Minimally, there should be logical separation, so that digital signature is activated by its own dedicated PIN. Otherwise, a cardholder will have no certainty after a PIN presentation whether whether a digital signature was generated. Providing a dedicated digital signing PIN moves control and protection of digital signatures from untrusted computer systems back to the cardholder.

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)
4	RU Consulting	Rick Uhrig	G	Not Present	**Consolidated PIV Repository**. Te Federal Government hasa legitimate need to quickly and conveniently determine who it has issued secure PIV credentials to. Example 1: Searching to see if a newly identified terrorist has been issued a PIV. Example 2: Detecting an Applicant who already has been issued a PIV or has recently had one revoked. A central repository could also ease the management of CRLs (a single federal source) and ease system availability requirements for each issuer PIV system. FIPS 201 does not state any policy or requirement for aggregating PIV issuance and revocation information.
5	RU Consulting	Rick Uhrig	G	D1 Throughout	**Presentation, Format & Content.** Much of FIPS 201, perhaps 70% to 80%, has more to do with background information, rationale, implementation guidance and agency specific procurement requirements than with actually establishing a PIV standard for secure and reliable forms of identification. With a few changes, this document could be streamlined and made substantially more useable for implementing departments and agencies, vendors, procurement officials, application developers, and conformance testers.

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)
6	RU Consulting	Rick Uhrig	G	D1 Throughout	**Document Organization**. The document could be reorganized along the lines of major components and processes in the lifecyle. Each should be a major section.
7	RU Consulting	Rick Uhrig	G	Crypto Sections	**First Use Dates for Crypto**. The PUBLIC Draft has last use dates for each algoeithim, but no first use dates. Effectively, this means an issuer can issue cards with any of the named algorithms, so that the PIV infratucture systems must support ALL the potential cryprto algorithms from day one. This is not feasible. A phase in period is need for new algorithms.
8	RU Consulting	Rick Uhrig	G	D1 Throughout	**Authentication Confusion.** FIPS 201 PUBLIC Draft Generall does not clearly distinguish between Authenticating the card, authenticating the cardholder by the card, and authenticating the cardholder by an external system. These ashould be clarified.

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)

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

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

Submitted by: _____

Date: _____

Proposed change
Provide graduated criteria as follows: a. Identity proofing b.1 Physical resistance to fraud & tampering b.2 Electrical resistance to fraud & tampering c.1 Electronic PIV authentication c.2 Electronic cardholder authentication d. Issuance See sample graduated criteria in associated file.
Include accreditation requirements. Minimally, these should include requirements for personnel, physical, procedural, and audit security. Protection of blank cardstock must be included. These should be included in the graduated criteria, to meet the security and functional needs of different issuers and to support a phase in period.

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

Submitted by: _____

Date: _____

Proposed change
In order of preference: 1. Physically isolate digital signature to a completely different chip card (well that isn't going to happen) 2. Require all PIV cards to implement logical separation by having a distinct PIN for digital signature 3. Rewrite FIPS 201 to be explicitly allow the card to have multiple PINs and a dedicated digital signing PIN. Allow card issuers to implement logical separation by having a distinct PIN for digital signature.

Submitted by: _____

Date: _____

Proposed change
Explicitly identify a consolidated PIV repository and requirements for issuers to provide transactions for each PPIV issued and revoked.
Extract text not related to setting of the standards, and make that available separately as background, rationale, and/oridance documents Consolidate free text to tables – for concision, clarity, and completeness – as is possible and reasonable See attached example of how FIPS 201 PUBLIC Draft was consolidated.

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

Submitted by: _____

Date: _____

Proposed change
Consider making each of the following its own major section in FIPS 201: • Identity Proofing • Issuance • Electronic Authentication • Card Requirements • Cryptography • Biometrics • Data Model • Chain of Trust
Add "first use" dates for each crypto algorithm and key size, so that the infrastructure support requirements will be clearly documented.
Clarify. See examples in attached documents.

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

Submitted by: _____

Date: _____

Proposed change

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