| 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 | Federal Reserve Board | | G | Section 1.3 | The latest release of the draft has broken out the PIV project into two phases. PIV-I identifies the minimum requirements for the PIV to be compliant with HSPD-12, leaving the interoperability between agencies to a future release of PIV. I believe the development of a PIV minimum 'checklist' would be of great benefit for agencies to utilize in determining compliance for each phase of this project. | Compliancy checklist |
| 2 | Federal Reserve Board | | G | Section 2.1 | An area of concern from a deployment concern by the October deadline is the final bullet that identifies 'credentials for physical and logical access to federally controlled facilities and information systems'. There needs to be clarity if the intention is for each agency to have deployed a fully vetted internal central PKI infrastructure ( or trusted external service) to meet this requirement. | Development of a pre-requisite checklist for FIPS 201 compliance. |
| 3 | Federal Reserve Board | | T | Section 2.2.1 | The Federal Reserve Board has an additional form to the ones listed in Table 2-1: Background Information Forms Required from Applicant. If the employee is filling a position with access to information classified for national security reasons, then SF-86 is completed and sent to OMB. | Consider inclusion of SF-86 form in table 2-1. |

| 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 |
|---|---|---|---|---|---|---|
| 4 | Federal Reserve Board | | G | Section 2.2.3 | If employees are not assigned a badge until a background investigation is complete, I'm assuming a temporary badge can be assigned for institutions that have implemented a two-factor authentication system for logical access so that basic services can be provided to the new employee, i.e. electronic mail. | Is there a distinction for physical and logical access for this section? If so, would be helpful to detail these environments. |
| 5 | Federal Reserve Board | | G | Section 3.2.1 | This section should also contain a bullet for 'on-going PIV maintenance'. This would include a strategy for providing physical and logical access to employees who lost or forgot their IDs on a given day. | Recommend acknowledgement of this issue in the standard. |
| 6 | Federal Reserve Board | | G | Section 3.3 | Breaks the PIV system into two logical subsystems. It would be helpful to understand if all or parts of these functional components are expected to be included in the PIV-I phase. | Would be helpful to understand the requirements for PIV-I from the components listed to ensure Octobor 2005 compliancy. |
| 7 | Federal Reserve Board | | G | Section 4.1.4.1 | There are questions raised whether noting "U.S. Government" on the card is a mandatory, since the agency seal is on the card. | Agency seal as mandatory and "U.S. Government" as optional text. |
| 8 | Federal Reserve Board | | E | Section 5 | This section covers an important aspect of a PIV and PKI implementation, the deployment of a CRL. It would be helpful to describe the intended use the CRL and the OCSP earlier in this section. It's my understanding that the OCSP service provides web-based ID verification that the badge has not been terminated as badges are verified by the human eye. | One sentenance description OCSP as beginning of Section 5. |

| 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 | Federal Reserve Board | | G | Section 6.3.1 | This section defines PIV logical access for "untrusted network connects". Is this the only logical access point requiring PIV controlled access? If not, this section could be a little misleading. If so, this needs to be highlighted in greater detail in the overview section of the standard. | Greater detail for logical access points if it extends past untrusted network connection points. |
| 10 | Federal Reserve Board | | T | Section 6 | The overall scope of FIPS 201 in the logical access arena is drawing the majority of comments within the Federal Reserve Board. These concerns are directly tied to the critical relationship between the Federal Reserve Board (a federal institution) and the twelve Federal Reserve Banks (non-federal institutions). Application and data sharing are intertwined between the Board and the twelve Banks. Therefore, a significant and unique hurdle in the development and adoption of a new authentication solution between these institutions could complicate the compliancy of FIPS 201. Moreover, the Board shares supervisory information and systems with state agencies. | FIPS 201 should address sharing of secure data with non-Federal agencies. |