Attachment 2
Submitted by: Steve Malphrus, Board of Governors of the Federal Reserve System
Date: December 22, 2004

General Comments on
Public Draft FIPS 201 NIST

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.

Section 2.1

This section is focused on ensuring that the registration authority at the Federal Reserve Board is reliably identified. These goals are certainly obtainable by the October 2005 deadline. An area of concern for a deployment 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 public key KI infrastructure (PKI) (or trusted external service) to meet this requirement

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 the Office of Personnel Management.

Section 2.2.3

If employees are not assigned a badge until a background investigation is complete, we are 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, e.g. electronic mail.

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.

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.

Section 4.1.4.1

We believe that the phrase "U.S. Government" should not be a mandatory statement on the card, since it will have the agency seal.

Section 5

This section covers an important aspect of a PIV and public key infrastructure (PKI) implementation, the deployment of a Certificate Revocation List (CRL). It would be helpful to describe the intended use the CRL and the Online Certificate Status Protocol (OCSP) earlier in this section. It is our 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.

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.

Other Comments

The overall scope of FIPS 201 in the logical access arena concerns us, because this is directly tied to the critical relationship between the Federal Reserve Board an independent federal agency and the twelve Federal Reserve Banks (private-sector 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 becoming compliant with of FIPS 201. Moreover, the Board shares supervisory information and systems with state banking commissioners (for state chartered banks) agencies. It would be helpful if FIPS 201 addresses sharing of secure data with non-federal entities.