GSA Office of Governmentwide Policy

December 06, 2006

MEMORANDUM FOR FEDERAL INFORMATION
SYSTEM SECURITY MANAGERS

FROM: Mary J. Mitchell
Deputy Associate Administrator for Technology Strategy

SUBJECT: Recognition of Certification and Accreditation of Certified PKI Shared Service Providers across Agency Boundaries

The General Services Administration (GSA) performs Certification and Accreditation (C&A) for Federal Public Key Infrastructure (PKI) Certified Shared Service Providers (SSP) as a part of the SSP evaluation process. Agencies are strongly encouraged to accept the results of this C&A when preparing for their own Federal Information Security Management Act (FISMA) compliance.

The Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification for Federal Employees and Contractors* for Homeland Security Presidential Directive (HSPD) 12, requires Federal agencies to acquire the services of a Certified PKI SSP. The Certified PKI SSP program was established to assist agencies in the decision making process when selecting a PKI service provider. As a service to agencies, GSA's Office of Governmentwide Policy certifies and accredits each Certified PKI SSP and issues an Authorization To Operate (ATO) upon successful review of supporting documentation.

As with all Federal information systems, these PKI SSPs must comply with FISMA which requires meeting mandatory minimum security requirements in accordance with FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.* In addition, the security controls in the Federal information system must be assessed for effectiveness as part of a formal C&A process in accordance with NIST Special Publication 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*.

Each agency is responsible for the C&A of any agency information system that interconnects with the Certified PKI SSP. The accreditation boundary of the agency

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

information system does not include the Certified PKI SSP information system. The GSA C&A can be accepted by each agency utilizing a Certified PKI SSP as assurance that the risk to the agencies' operations, assets, and to individuals arising from the use of the Certified PKI SSP is at an acceptable level of risk in accordance with NIST Special Publication 800-53 guidance on the use of external information system services and service providers.

Agencies acquiring the services of a Certified PKI SSP to comply with HSPD-12 can use the results of the GSA C&A in making their own risk determination as part of the agency C&A of their HSPD-12 implementation. GSA will share Certified PKI SSP C&A documentation with the Information System Security Officers (ISSO) of requesting agencies to aid them completing their agency C&A on this interconnecting information system. Leveraging the C&A conducted by GSA will allow participating Federal agencies to achieve significant cost avoidance and greater consistency in the application of security controls within the information system managed and operated by their Certified PKI SSP.

For additional information, please contact Judith Spencer in the GSA Office of Governmentwide Policy at judith.spencer@gsa.gov.