CI-FSS-052 AUTHENTICATION PRODUCTS AND SERVICES (JAN 2010)

(a) General Background.

(1) The General Services Administration (GSA) originally established the Access Certificates for Electronic Services (ACES) Program to provide digital certificates and PKI services for enabling e-Government applications that require logical access control, digital signature and/or electronic authentication. The ACES Program provided for the issuance of electronic credentials to individuals and entities external to the Federal Government. The Federal PKI Policy Authority approved the policies and requirements of the ACES Program to satisfy the Federal requirements for cross-certification with the Federal Bridge Certification Authority (FBCA) and participation in the Federal e-Authentication initiative. The term ###Identity and Access Management### (IAM) is now being used to clearly define the kinds of services that meet the requirements for service providers and products that support FISMA-compliant IAM systems deployed by federal agencies. In addition, many states have adopted corresponding standards for IAM.

(2) Homeland Security Presidential Directive 12 (HSPD-12), ###Policy for a Common Identification Standard for Federal Employees and Contractors### establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractor employees assigned to Government contracts in order to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. Further, the Directive requires the Department of Commerce to promulgate a Federal standard for secure and reliable forms of identification within six months of the date of the Directive. As a result, the National Institute of Standards and Technology (NIST) released Federal Information Processing Standard (FIPS) 201: Personal Identity Verification of Federal Employees and Contractors on February 25, 2005. FIPS 201 requires that the digital certificates incorporated into the Personal Identity Verification (PIV) identity credentials comply with the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework. In addition, FIPS 201 requires that Federal identity badges referred to as PIV credentials, issued to Federal employees and contractors comply with the Standard and associated NIST Special Publications 800-73, 800-76, 800-78, and 800-79.

(b) Special Item Numbers.

The General Services Administration has established the e-Authentication Initiative (see URL: http://www.idmanagement.gov) to provide common infrastructure for the authentication of the public and internal federal users for logical access to Federal e-Government applications and electronic services. To support the government-wide implementation of HSPD-12 and the Federal e-Authentication Initiative, GSA has established Special Item Numbers (SINs) pertaining to Authentication Products and Services, including Electronic Credentials, Digital Certificates, e-Authentication, Identify and Access Management, PKI Shared Service Providers, and HSPD-12 Product and Service Components.

(c) Qualification Information.

(1) All Authentication Products and Services must be qualified as being compliant with Government-wide requirements before they will be included on a GSA Information Technology (IT) Schedule contract. The Qualification Requirements and associated evaluation procedures against the Qualification Requirements for each SIN and the specific Qualification Requirements for HSPD-12 implementation components are presented at the following URL: http://www.idmanagement.gov.

(2) In addition, the National Institute of Standards and Technology (NIST) has established the NIST Personal Identity Verification Program (NPIVP) to evaluate integrated circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform card and reader interface testing for interoperability. Products that are approved as FIPS-201 compliant through these evaluation and testing programs may be offered directly through the HSPD-12 Product and Services Components SIN, under the category ###Approved FIPS 201-Compliant Products and services###.

(d) Qualification Requirements.

(1) Offerors proposing Authentication products and services under the established Special Item Numbers (SINs) are required to provide the following:

(i) Proposed items must be determined to be compliant with Federal requirements for that Special Item Number. Qualification Requirements and procedures for the evaluation of products and services are posted at the URL: http://www.idmanagement.gov. GSA will follow these procedures in qualifying offeror###s products and services against the Qualification Requirements for applicable to SIN. Offerors must submit all documentation certification letter(s) for Authentication Products and Services offerings at the same time as the submission of proposal. Award will be dependent upon receipt of official documentation from the Acquisition Program Management Office (APMO) listed below verifying satisfactory qualification against the Qualification Requirements of the proposed SIN(s).

(ii) After award, Contractor agrees that certified products and services will not be offered under any other SIN on any GSA Multiple Award Schedule.

(iii)############(A) If the Contractor changes the products or services previously qualified, GSA
may require the contractor to resubmit the products or services for re-qualification.

(B) If the Federal Government changes the qualification requirements or standards, Contractor must resubmit the products and services for re-qualification.

(2) Immediately prior to making an award, Contracting Officers MUST consult the following website to ensure that the supplies and/or services recommended for award under any Authentication Products and Services SINs are in compliance with the latest APL qualification standards: www.idmanagement.gov . A dated copy of the applicable page should be made and included with award documents.

(e) Demonstrating Conformance.

(1) The Federal Government has established Qualification Requirements for demonstrating conformance with the Standards. The following websites provide additional information regarding the evaluation and qualification processes:

(i) For Access Certificates for Electronic Services (ACES) and PKI Shared Service Provider (SSP) Qualification Requirements and evaluation procedures: http://www.idmanagement.gov;

(ii) For HSPD-12 Product and Service Components Qualification Requirements and evaluation procedures: http://www.idmanagement.gov;

(iii) For FIPS 201 compliant products and services qualification and approval procedures: http://www.csrc.nist.gov/piv-project/ and http://www.smart.gov .

(f) Acquisition Program Management Office (APMO).

GSA has established the APMO to provide centralized technical oversight and management regarding the qualification process to industry partners and Federal agencies. Contact the following APMO for information on the e-Authentication Qualification process. Technical, APMO, FIPS 201and HSPD-12 Points of Contacts can be found below, or in an additional attachment to the Solicitation.

See Attachment