552.238-109 Authentication Supplies and Services.

As prescribed in 538.273 (d)(33) insert the following clause:

Authentication Supplies and Services (May 2019)

(a) *General background.*

(1) The General Services Administration (GSA) established the "Identity and Access Management Services" (IAMS) Program to clearly define the kinds of digital certificates and PKI services that meet the requirements for service providers and supplies that support FISMA-compliant IAM systems deployed by Federal agencies.

(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) 201-2: Personal Identity Verification of Federal Employees and Contractors August 2013. FIPS 201-2 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 201-2 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. GSA 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, eAuthentication, Identify and Access Management, PKI Shared Service Providers, and HSPD-12 Product and Service Components.

(c) *Qualification information.*

(1) All Authentication supplies 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

supplies against conformance requirements contained in FIPS 201. GSA has established the FIPS 201Evaluation Program to evaluate other supplies 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 HSPD-12 Supplies and Services Components SIN under the category “Approved FIPS 201-Compliant Products and services.

(d) *Qualification requirements*. Offerors proposing Authentication supplies and services under the established SINs are required to provide the following:

(1) Proposed items must be determined to be compliant with Federal requirements for that SIN. Qualification Requirements and procedures for the evaluation of supplies and services are posted at the URL: http://www.idmanagement.gov. GSA will follow these procedures in qualifying offeror's supplies and services against the Qualification Requirements for applicable to SIN. Offerors must submit all documentation certification letter(s) for Authentication Supplies and Services offerings at the same time as 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).

(2) After award, Contractor agrees that certified supplies and services will not be offered under any other SIN on any Federal Supply Schedule

(3)

(i) If the Contractor changes the supplies or services previously qualified, GSA may require the Contractor to resubmit the supplies or services for re-qualification.

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

(4) 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 Supplies 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 the 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 Identify and Access Management Services (IAMS) 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 evaluation program testing and certification procedures: https://www.idmanagement.gov/fips201/.

(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 eAuthentication Qualification process. Technical, APMO, FIPS 201, and HSPD-12 Points of Contact can be found below, or in an additional attachment to the solicitation.

[*The contracting officer should insert the points of contact information below, unless otherwise included elsewhere in the solicitation.*]

____

(End of clause)

Parent topic: 552.238 [Reserved]