

**Solicitation FCIS-JB-980001-B
FSC Group 70
SIN 132-62**

**Homeland Security Presidential Directive (HSPD-12)
Product and Service Components**

**Personal Identity Verification (PIV) Systems
Infrastructure Services and Products**

Statement of Qualification Requirements

Date: June 19, 2006

Revised: August 30, 2006

GSA

U.S. General Services Administration

Federal Acquisition Service

Change Control Page

| Date | Description |
|-----------|--|
| 6/19/2006 | Initial release of the PIV Qualification Requirements |
| 8/30/2006 | Revised Appendix A to require submission of completed compliance matrix. |
| | |
| | |
| | |
| | |
| | |

TABLE OF CONTENTS

| | | |
|--------------|---|-----------|
| 1.0 | Overview | 1 |
| 1.1 | Background | 1 |
| 1.2 | Objectives | 2 |
| 2.0 | PIV Card System Description..... | 3 |
| 2.1 | Enrollment and Registration Services and Products..... | 4 |
| 2.2 | PIV Systems Infrastructure Services and Products | 4 |
| 2.3 | PIV Card Management and Production Services and Products | 4 |
| 2.4 | PIV Card Activation and Finalization Services and Products | 4 |
| 2.5 | Physical Access Control Services and Products..... | 4 |
| 2.6 | Logical Access Control Services and Products | 4 |
| 2.7 | PIV System Integration Services and Products | 5 |
| 2.8 | Approved FIPS 201-Compliant Services and Products | 5 |
| 2.9 | Professional Services..... | 5 |
| 2.10 | PIV Associated Systems..... | 5 |
| 2.10.1 | Agency-Specific IDMS..... | 5 |
| 2.10.2 | OPM/Federal Bureau of Investigation (FBI) | 5 |
| 2.11 | PIV Roles | 5 |
| 2.12 | Conceptual Overview of PIV Components..... | 6 |
| 2.13 | PIV Systems Infrastructure Components..... | 7 |
| 3.0 | PIV Systems Infrastructure Services and Products Qualification Requirements..... | 8 |
| 3.1 | Scope and Description of Qualification Requirements | 9 |
| 3.1.1 | Systems Infrastructure Hardware and Software Products | 11 |
| 3.1.1.1 | Technical Standards Compliance..... | 16 |
| 3.1.1.2 | Interface and Interoperability Support..... | 16 |
| 3.1.1.3 | Systems Infrastructure Software | 17 |
| 3.1.1.4 | Security Standards Compliance | 17 |
| 3.1.1.5 | Hardware and Software Maintenance Support | 17 |
| 3.1.1.6 | Special Contract Requirements..... | 17 |
| 3.1.1.7 | Allowance for Technology Changes..... | 17 |
| 3.1.1.8 | Contractor Personnel Training..... | 18 |
| 3.1.1.9 | Administrative and Personnel Security..... | 19 |
| 3.1.1.10 | Deliverables | 19 |
| 3.1.1.11 | Hardware and Software Products Qualification Requirements Response Package Submission..... | 21 |
| 3.1.2 | Systems Infrastructure Deployment Services | 22 |
| 3.1.2.1 | Systems Infrastructure Hardware and Software Compliance | 22 |

| | | |
|--------------|---|-----------|
| 3.1.2.2 | Training..... | 23 |
| 3.1.2.3 | Customer Service Center | 23 |
| 3.1.2.4 | Special Contract Requirements..... | 25 |
| 3.1.2.5 | Availability of Services | 25 |
| 3.1.2.6 | Response Time for Services..... | 25 |
| 3.1.2.7 | Scalability and Implementation Schedule..... | 25 |
| 3.1.2.8 | Allowance for Technology Changes..... | 26 |
| 3.1.2.9 | Past Performance | 26 |
| 3.1.2.10 | Contractor Personnel Training..... | 27 |
| 3.1.2.11 | Administrative and Personnel Security..... | 27 |
| 3.1.2.12 | Deliverables | 27 |
| 3.1.2.13 | Project Management Office | 30 |
| 3.1.2.14 | Deployment Services Qualification Requirements Response Package Submission | 30 |
| 3.1.3 | Managed Systems Infrastructure Services | 31 |
| 3.1.3.1 | Systems Infrastructure Hardware and Software Compliance | 31 |
| 3.1.3.2 | Systems Infrastructure Deployment Services Compliance..... | 31 |
| 3.1.3.3 | IDMS, CMS and Business Process Management Services Compliance | 31 |
| 3.1.3.4 | PIV Lifecycle Management | 32 |
| 3.1.3.5 | Revocation and Termination..... | 32 |
| 3.1.3.6 | Renewal..... | 33 |
| 3.1.3.7 | Replacement..... | 34 |
| 3.1.3.8 | Re-issuance | 34 |
| 3.1.3.9 | Card Lifecycle Management Interactions..... | 35 |
| 3.1.3.10 | Audit, Logging, and Standard Reporting..... | 35 |
| 3.1.3.11 | Technical Standards Compliance..... | 36 |
| 3.1.3.12 | Interface and Interoperability Support..... | 37 |
| 3.1.3.13 | Security C&A and Re-Accreditation | 38 |
| 3.1.3.13.1 | <i>Plan for Completion of Initial C&A</i> | <i>38</i> |
| 3.1.3.13.2 | <i>Periodic Review of Security Controls.....</i> | <i>39</i> |
| 3.1.3.14 | Date/Time Stamp Synchronization | 39 |
| 3.1.3.15 | Performance | 39 |
| 3.1.3.15.1 | <i>Hours of Operation.....</i> | <i>39</i> |
| 3.1.3.15.2 | <i>Availability of Services</i> | <i>40</i> |
| 3.1.3.15.3 | <i>Response Time for Services.....</i> | <i>40</i> |
| 3.1.3.16 | Customer Service Center | 40 |
| 3.1.3.16.1 | <i>Services for Ordering Activity Applications.....</i> | <i>40</i> |
| 3.1.3.16.2 | <i>Card Holder Services.....</i> | <i>41</i> |
| 3.1.3.16.3 | <i>Hours of Operation.....</i> | <i>41</i> |
| 3.1.3.16.4 | <i>Toll-free Telephone Service</i> | <i>41</i> |
| 3.1.3.16.5 | <i>On-line and E-Mail Services.....</i> | <i>42</i> |
| 3.1.3.16.6 | <i>Problem Identification and Resolution.....</i> | <i>42</i> |

| | | |
|---|---|-----------|
| 3.1.3.16.7 | <i>Customer Service Records</i> | 42 |
| 3.1.3.17 | Privacy Act Requirements | 43 |
| 3.1.3.18 | Contractor Personnel Training..... | 43 |
| 3.1.3.19 | Data Transfer | 43 |
| 3.1.3.20 | Security/Privacy Requirements..... | 43 |
| 3.1.3.20.1 | <i>Administrative and Personnel Security</i> | 44 |
| 3.1.3.20.2 | <i>Privacy Requirements</i> | 44 |
| 3.1.3.20.3 | <i>Data Retention</i> | 44 |
| 3.1.3.21 | Past Performance | 44 |
| 3.1.3.22 | Deliverables | 45 |
| 3.1.3.23 | Project Management Office | 49 |
| 3.1.3.24 | Systems Infrastructure Services Qualification Requirements Response Package Submission | 49 |
| 3.2 | Pricing | 51 |
| Appendix A: Qualification Requirements Submission Criteria | | 1 |

List of Tables

| | |
|---|-----------|
| Table 3.1-1. List of Systems Infrastructure Services and Products Qualification Requirements | 9 |
| Table 3.1.1.10-1. Deliverables | 19 |
| Table 3.1.2.6-1. Response Time Requirements | 25 |
| Table 3.1.2.12-1. Deliverables | 27 |
| Table 3.1.3.15.3-1. Response Time Requirements | 40 |
| Table 3.1.3.22-1. Deliverables | 45 |

List of Figures

| | |
|---|----------|
| Figure 2.12-1. Conceptual Overview of PIV Components | 7 |
| Figure 2.13-1. PIV Systems Infrastructure Components | 7 |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

1.0 Overview

General Services Administration (GSA), Federal Acquisition Service (FAS) requires the Contractor to provide the supplies and services necessary to support a common, interoperable, multi-application HSPD-12 PIV card solution as specified in this document. The HSPD-12 PIV program allows Federal agencies, activities, and organizations to select from multiple and flexible solutions to meet HSPD-12 PIV requirements. The Contractor will be called upon to provide HSPD-12 PIV compliant services and products under individual task/delivery orders issued in accordance with FSC Group 70 Special Item Numbers (SIN):

- 132-60, Access Certificates for Electronic Services (ACES) Program (SIN 132-60).
- 132-61, PKI Shared Service Providers (PKI SSP) Program (SIN 132-61).
- 132-62, HSPD-12 Product and Service Components (SIN 132-62).

This Statement of Qualification Requirements establishes the qualification requirements for providing PIV Systems Infrastructure Services and Products under SIN 132-62, HSPD-12 Product and Service Components.

1.1 Background

Authentication services and products provide for authentication of individuals for purposes of physical and logical access control, electronic signature, and performance of E-business transactions and delivery of Government services. Authentication products and services consist of hardware, software components and supporting services that provide for identity assurance.

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 201: Personal Identity Verification of Federal Employees and Contractors (FIPS 201) on February 25, 2005. FIPS 201 requires that the digital certificates incorporated into the 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.

HSPD-12 requires that the Federal credential (the PIV card) be secure and reliable, which is defined as a credential that:

- Is issued based on sound criteria for verifying an individual's identity.

- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation.
- Can be rapidly authenticated electronically.
- Is issued only by providers whose reliability has been established by an official accreditation process.

In support of this goal, GSA's Office of Governmentwide Policy (OGP) and FAS share responsibility for the design, development, implementation, operation, and maintenance of the HSPD-12 PIV Program.

This Statement of Qualification Requirements under FSC Group70, SIN 132-62, provides the specification of minimum technical functions and capabilities related to the HSPD-12 PIV systems infrastructure services and products. Contractors must meet the qualification requirements as specified in order to be considered for contract award under SIN 132-62 for HSPD-12 PIV systems infrastructure services and products. HSPD-12 PIV systems infrastructure services and products provide for authentication of individuals for purposes of physical and logical access controls, electronic signature, performance of E-business transactions, and delivery of government services.

At a minimum, the ordering organization can use an HSPD-12 PIV card as a Federal employee or agency Contractor requiring physical and logical access to Federal facilities and networks. The Contract under SIN 132-62 offers the vehicle to issue PIV cards that can be used to provide basic visual identification, electronic identification and authentication for physical and logical access control, cryptographic services, biometrics functions, as well as a number of value added features. The PIV card contains information carried on a processing chip that could be used commonly across applications.

1.2 Objectives

The objectives of the HSPD-12 PIV services and products are to:

- (1) Achieve best value for PIV cards and services by aggregating Government requirements.
- (2) Provide government agencies and other ordering activities with robust PIV services.
- (3) Achieve maximum efficiency by procuring PIV services from existing commercially available products, systems, and services, to the extent possible.
- (4) Achieve maximum efficiency in procuring PIV services by encouraging partnership arrangements among commercial entities.
- (5) Achieve implementation of a trust model which features.

- (6) Use of a single PIV card and PIV digital credentials for physical and logical access to Government facilities and information systems.
- (7) Quality assurance and inspection of Contractor's practices for adherence to terms of HSPD-12 and FIPS 201.
- (8) Achieve intra-operability among the functional components within an enterprise PIV services solution and interoperability across Government implementations by defining a set of standard methods for issuing and accessing standard PIV card data in accordance with FIPS 201 and related technical specifications ¹.

2.0 PIV Card System Description

The PIV card system as described will provide the security, privacy, and interoperability as required in HSPD-12 and FIPS 201. The HSPD-12 implementation components specified under SIN 132-62 are as follows:

- PIV enrollment and registration services and products.
- PIV systems infrastructure services and products.
- PIV card management and production services and products.
- PIV card activation and finalization services and products.
- Physical access control services and products.
- Logical access control services and products.
- PIV system integration services and products.
- Approved FIPS 201-compliant services and products.
- Professional services to support implementation and integration for ordering activities and applications.

The PIV categories of systems, products, and services are those that are required to manage users and their cards through the entire PIV card life cycle. Associated systems include those that interact with the system and either provide information or use information from the system, such as the Office of Personnel Management (OPM) in checking the suitability of applicant information provided by the registration/enrollment system and agency Identity Management Systems (IDMS) that provide access control and other identity information specific to agency requirements.

¹ All references to FIPS 201 throughout this document incorporate references to the latest release versions of FIPS 201 and all related NIST Special Publications and technical specifications.

Summary definitions of the categories of PIV systems, products, and services are provided in the following sections.

2.1 Enrollment and Registration Services and Products

The enrollment and registration services and products relate to the process of collecting identity information from a PIV applicant and distributing that information to other component systems and services within the PIV system, such as the PIV systems infrastructure. The applicant will be “sponsored” by a government employee. Systems infrastructure functions will be provided via processes that enable the enrollment and registration to be “local” to the applicant.

2.2 PIV Systems Infrastructure Services and Products

The PIV systems infrastructure services and products relate to provision of a set of business process functions that manages the PIV workflow among and between other PIV system components. Specifically, PIV systems infrastructure services and products provide the software functionality required to manage PIV credentials, including IDMS and Card Management Systems (CMS).

2.3 PIV Card Management and Production Services and Products

The PIV card management and production services and products relate to card lifecycle management, including card production, personalization, printing, internal configuration for use, and delivery of the card for finalization and issuance.

2.4 PIV Card Activation and Finalization Services and Products

The PIV card activation and finalization services relate to final issuance of the PIV card to the applicant including verification of identity of the applicant, verification of PIV card operation, final configuration of Public Key Infrastructure (PKI) components, and obtaining signatures from the applicant verifying receipt of the card.

2.5 Physical Access Control Services and Products

The physical access control services and products and products relate to the provision of the functions required to provide card holders with access to government controlled facilities. The physical access control services and products interface directly and indirectly with other PIV system components and agency-specific systems.

2.6 Logical Access Control Services and Products

The logical access control services and products relate to provision of the functions required to provide card holders with access to government controlled IT networks and computer systems. The logical access control services and products interface directly and indirectly with other PIV system components and agency-specific systems.

2.7 PIV System Integration Services and Products

The PIV system integration services products relate to provision of integrated PIV system components, products, and services. It also relates to integration of PIV system components with existing agency systems and infrastructures.

2.8 Approved FIPS 201-Compliant Services and Products

Approved FIPS 201-compliant services and products relate to provision of services and products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. 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 201 Evaluation 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.

2.9 Professional Services

Professional services relates to provision of support for implementation and integration for ordering activities and applications.

2.10 PIV Associated Systems

2.10.1 Agency-Specific IDMS

Agency-specific Identity Management Systems (IDMS) will maintain access control and other identity information as may be required by the agency to manage physical and logical access to the agency.

2.10.2 OPM/Federal Bureau of Investigation (FBI)

All PIV applicant background investigations will be conducted through the OPM. The OPM will conduct the investigations and forward results to the appropriate agency and/or PIV system component. The Federal Bureau of Investigation will be responsible for conducting fingerprint checks against its fingerprint databases as a component of all background investigations and will interface directly and indirectly with OPM and the appropriate PIV system component.

2.11 PIV Roles

The following roles are used throughout this Statement of Qualification Requirements to describe individuals who perform PIV functions:

- (1) **Applicant** - The individual to whom a PIV credential needs to be issued.
- (2) **PIV Sponsor** - The individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.
- (3) **Enrollment Official** - The entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant.
- (4) **Issuer** - The entity that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.
- (5) **PIV Digital Signatory** - The entity that digitally signs the PIV biometrics and CHUID.
- (6) **PIV Authentication Certification Authority (CA)** - The CA that signs and issues the PIV Authentication Certificate.

The principle of separation of duties will be enforced to ensure that no single individual has the capability to issue a PIV card without the participation of another authorized person. The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.

2.12 Conceptual Overview of PIV Components

Figure 2.12-1, Conceptual Overview of PIV Components, provides a high-level overview of the PIV components and functionalities. At the time of implementation and based on agency requirements, the order of the functions and processes may differ from the numbered order illustrated.

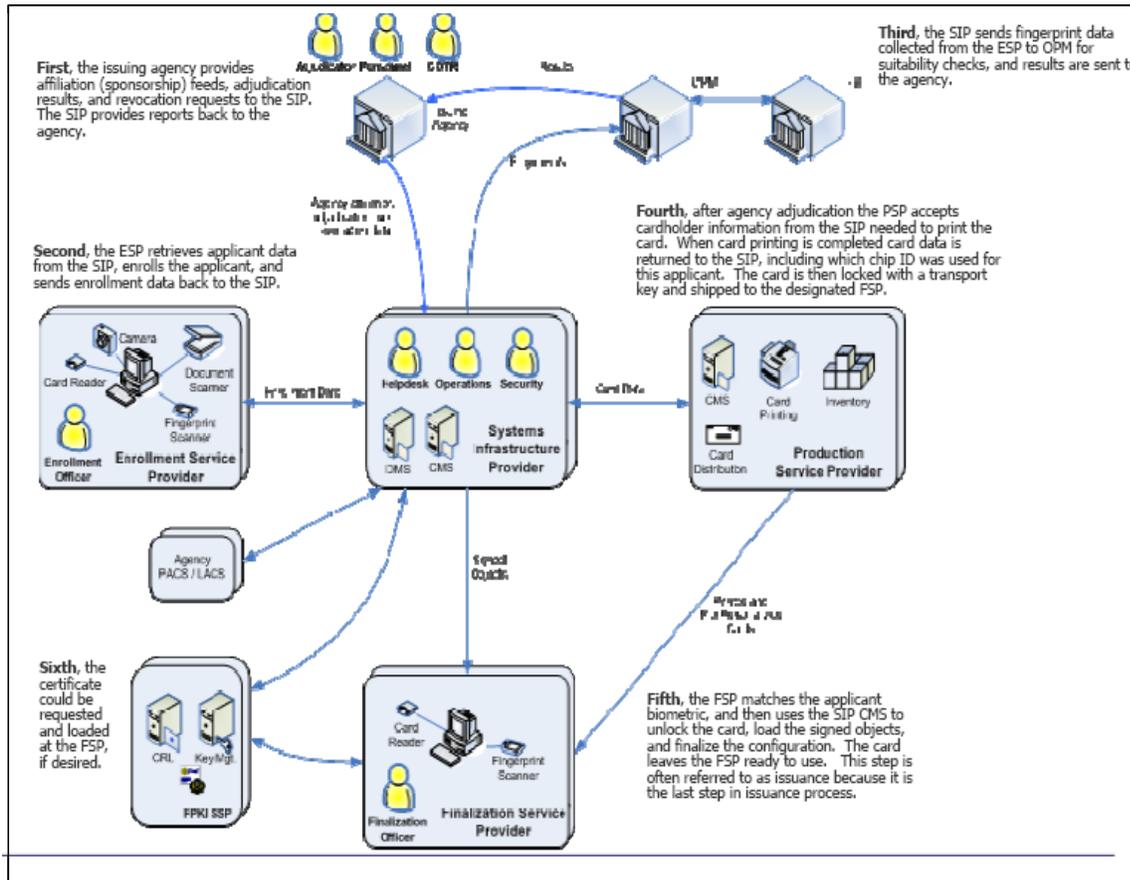


Figure 2.12-1. Conceptual Overview of PIV Components

2.13 PIV Systems Infrastructure Components

Figure 2.13-1, PIV Systems Infrastructure Components, depicts the components that incorporate the scope of the qualifications document.

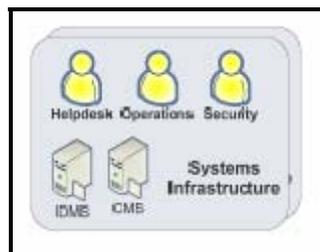


Figure 2.13-1. PIV Systems Infrastructure Components

3.0 PIV Systems Infrastructure Services and Products Qualification Requirements

This Statement of Qualification Requirements under FSC Group 70, SIN 132-62, provides the specification of minimum technical functions and capabilities related to the provision of HSPD-12 PIV systems infrastructure services and products. Contractors must meet the qualification requirements as specified in order to be considered for contract award under SIN 132-62 for HSPD-12 PIV systems infrastructure services and products.

The Contractor shall have the capability to provide systems infrastructure of PIV applicants. The Contractor shall have the capability to provide the functionality to collect, store, and maintain all information and documentation required to verify and assure the applicant's identity. Source identity information (e.g., passport, driver's license) and various types of biometric data (e.g., fingerprints, photographs) shall be collected from the applicant at the time of registration, IAW FIPS 201.

The Contractor shall have the technical capability to provide one or more services and products in the following categories:

- (1) Systems infrastructure hardware and software products.
- (2) Systems infrastructure deployment services.
- (3) Managed Systems infrastructure services.

The Contractor shall have the capability to provide HSPD-12 PIV and GSA compliant services and products.

Contractors shall have the capability to provide individual hardware and software products and/or complete standard configuration systems infrastructure stations.

All services and products related to the PIV card for which compliance is required must comply with HSPD-12, FIPS 201, applicable NIST Special Publications and/or GSA interoperability compliance requirements. For categories of services and products that require GSA approval (see <http://fips201ep.cio.gov/index.php>), the Contractor shall deliver only solution components that have been certified by NIST and approved by GSA, as appropriate, when such components are commercially available.

Approved FIPS 201-compliant services and products relate to provision of services and products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. NIST has established the NPVCP to evaluate integrated circuit chip cards and products against conformance requirements contained in FIPS 201. GSA has established the FIPS 201 Evaluation 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.

3.1 Scope and Description of Qualification Requirements

The scope and descriptions of the qualification requirements for provision of HSPD-12 PIV systems infrastructure services and products are defined in the following sections. Table 3.1-1, List of Systems Infrastructure Services and Products Qualification Requirements, provides a list of the qualification requirements the Contractor shall address and indicates the applicable section reference for each item.

Table 3.1-1. List of Systems Infrastructure Services and Products Qualification Requirements

| Requirement No. | Description | Section References |
|--|---|---------------------------|
| Systems Infrastructure Hardware and Software Products | | |
| 1. | Technical Standards Compliance | 3.1.1.1 |
| 2. | Interface and Interoperability Support | 3.1.1.2 |
| 3. | Systems Infrastructure Software | 3.1.1.3 |
| 4. | Security Standards Compliance | 3.1.1.4 |
| 5. | Hardware and Software Maintenance Support | 3.1.1.5 |
| 6. | Special Contract Requirements | 3.1.1.6 |
| 7. | Allowance for Technology Changes | 3.1.1.7 |
| 8. | Contractor personnel Training | 3.1.1.8 |
| 9. | Administrative Personnel Security | 3.1.1.9 |
| 10. | Deliverables | 3.1.1.10 |
| 11. | Hardware and Software Products Qualification Requirements Response Package Submission | 3.1.1.11 |
| Systems Infrastructure Deployment Services | | |
| 12. | Systems Infrastructure Hardware and Software Compliance | 3.1.2.1 |
| 13. | Training | 3.1.2.2 |
| 14. | Customer Service Center | 3.1.2.3 |
| 15. | Special Contract Requirements | 3.1.2.4 |

| Requirement No. | Description | Section References |
|--|---|---------------------------|
| 16. | Availability of Services | 3.1.2.5 |
| 17. | Response Time for Services | 3.1.2.6 |
| 18. | Scalability and Implementation Schedule | 3.1.2.7 |
| 19. | Allowance for Technology Changes | 3.1.2.8 |
| 20. | Past Performance | 3.1.2.9 |
| 21. | Contractor Personnel Training | 3.1.2.10 |
| 22. | Administrative and Personnel Security | 3.1.2.11 |
| 23. | Deliverables | 3.1.2.12 |
| 24. | Project Management Office | 3.1.2.13 |
| 25. | Deployment Services Qualification Requirements Response Package Submission | 3.1.2.14 |
| Managed Systems Infrastructure Services | | |
| 26. | Systems Infrastructure Hardware and Software Compliance | 3.1.3.1 |
| 27. | Systems Infrastructure Deployment Services Compliance | 3.1.3.2 |
| 28. | IDMS, CMS, and Business Process Management Services | 3.1.3.3 |
| 29. | PIV Lifecycle Management | 3.1.3.4 |
| 30. | Revocation and Termination | 3.1.3.5 |
| 31. | Renewal | 3.1.3.6 |
| 32. | Replacement | 3.1.3.7 |
| 33. | Re-issuance | 3.1.3.8 |
| 34. | Card Lifecycle Management Interactions | 3.1.3.9 |
| 35. | Audit, Logging, and Standard Reporting | 3.1.3.10 |
| 36. | Technical Standards Compliance | 3.1.3.11 |
| 37. | Interface and Interoperability Support | 3.1.3.12 |
| 38. | Security Certification and Accreditation (C&A) and Re-Accreditation | 3.1.3.13 |

| Requirement No. | Description | Section References |
|------------------------|--|---------------------------|
| 39. | Date/Time Stamp Synchronization | 3.1.3.14 |
| 40. | Performance | 3.1.3.15 |
| 41. | Customer Service Center | 3.1.3.16 |
| 42. | Privacy Act Requirements | 3.1.3.17 |
| 43. | Contractor Personnel Training | 3.1.3.18 |
| 44. | Data Transfer | 3.1.3.19 |
| 45. | Security/Privacy Requirements | 3.1.3.20 |
| 46. | Past Performance | 3.1.3.21 |
| 47. | Deliverables | 3.1.3.22 |
| 48. | Project Management Office | 3.1.3.23 |
| 49. | Systems Infrastructure Services Qualification Requirements Response Package Submission | 3.1.3.24 |
| Pricing | | |
| 50. | Pricing | 3.2 |

3.1.1 Systems Infrastructure Hardware and Software Products

The Contractor shall have the capability to provide standard configuration systems infrastructure hardware and/or software products to be purchased and owned by an ordering entity (i.e., agency) that includes, the following functional requirements to capture, store, and maintain systems infrastructure information:

- (1) CMS: The Contractor shall have the capability to provide a CMS, including all hardware and/or software, that shall provide the following functionalities:
 - (a) Implementation of interfaces with other authorized PIV systems infrastructure components (i.e., IDMS, card management and production).
 - (b) Maintenance of card lifecycle information, from receipt of request to produce the PIV card, delivery of the activated and finalized PIV card to the card holder, and final disposition (i.e., lost, stolen, destroyed).
 - (c) Support for secure backup of all data related to card holder and card history information.
 - (d) Full operation and on-line availability 24 hours per day and seven days per week to accept card production requests, status updates, and for on-line

functions in support of other authorized PIV system services and other normal business functions.

- (e) Sufficient database capacity.
- (f) Access controls that permit only authorized and authenticated users and system transactions.
- (g) Storage and maintenance of the following card data:
 - (1) Mandatory card data:
 - (a) Photograph
 - (b) Name
 - (c) Employee Affiliation
 - (d) Organizational Affiliation
 - (e) Expiration Date
 - (f) Agency Card Serial Number
 - (g) Issuer Identification
 - (h) PIN
 - (i) Cardholder Unique Identifier (CHUID)
 - (j) PIV authentication certificate
 - (k) Biometric fingerprints
 - (l) PIV authentication certificate
 - (2) Operational card data:
 - (a) Cardholder signature
 - (b) Agency specific text
 - (c) Rank
 - (d) Portable Data File (PDF) Two-Dimensional Bar Code Information
 - (e) Header
 - (f) Agency Seal
 - (g) Footer
 - (h) Issue Date
 - (i) Color-Coding for Employee Affiliation
 - (j) Photo Border for Employee Affiliation
 - (k) Agency-Specific Data
 - (l) Return to Information
 - (m) Physical Characteristics of Cardholder
 - (n) Additional Language for Emergency Responder Officials
 - (o) Standard Section 499, Title 18 Language
 - (p) Linear 3 of 9 Bar Code information
 - (q) Agency-Specific Text
 - (r) Certificate for Digital Signatures
 - (s) Certificate for Key Management

- (t) Asymmetric or Symmetric Card Authentication Keys for Supporting PACS
- (u) Symmetric Key(s) associated with the CMS
- (g) Data maintenance, retention, and disposition capabilities IAW with the Federal laws, standards, regulations, and guidelines, including the Privacy Act of 1974.
- (h) Maintain a list of approved systems PIV system components (i.e., IDMS, Issuers) that can submit PIV requests for card product.
- (i) Provide acknowledgment of request to produce a PIV card.
- (j) Notify approved system infrastructure components upon completion of PIV card production.
- (k) Secure transmission and receipt of applicant data to provide for integrity and confidentiality of the data only from authorized PIV systems.
- (2) Identity Management System (IDMS): The Contractor shall have the capability to provide an identity management system (IDMS), including all hardware and software, that shall, at a minimum, provide the following:
 - (a) Maintenance of card holder lifecycle information, from application to delivery of the activated and finalized PIV card to the card holder, and final disposition (i.e., lost, stolen, destroyed).
 - (b) Support for secure backup of all data related to card holder and card history information.
 - (c) Full operation and on-line availability 24 hours per day and seven (7) days per week to accept card production requests, status updates, and for on-line functions in support of other authorized PIV system services and other normal business functions.
 - (d) Sufficient database capacity.
 - (e) Access controls that permit only authorized and authenticated users and system transactions.
 - (f) Storage and maintenance of the following card data:
 - (1) Mandatory card data:
 - (a) Photograph
 - (b) Name
 - (c) Employee Affiliation
 - (d) Organizational Affiliation
 - (e) Expiration Date

- (f) Agency Card Serial Number
 - (g) Issuer Identification
 - (h) PIN
 - (i) Cardholder Unique Identifier (CHUID)
 - (j) PIV authentication certificate
 - (k) Biometric fingerprints
 - (l) PIV authentication certificate
- (2) Optional card data:
- (a) Cardholder signature
 - (b) Agency specific text
 - (c) Rank
 - (d) Portable Data File (PDF) Two-Dimensional Bar Code Information
 - (e) Header
 - (f) Agency Seal
 - (g) Footer
 - (h) Issue Date
 - (i) Color-Coding for Employee Affiliation
 - (j) Photo Border for Employee Affiliation
 - (k) Agency-Specific Data
 - (l) Return to Information
 - (m) Physical Characteristics of Cardholder
 - (n) Additional Language for Emergency Responder Officials
 - (o) Standard Section 499, Title 18 Language
 - (p) Linear 3 of 9 Bar Code information
 - (q) Agency-Specific Text
 - (r) Certificate for Digital Signatures
 - (s) Certificate for Key Management
 - (t) Asymmetric or Symmetric Card Authentication Keys for Supporting PACS
 - (u) Symmetric Key(s) associated with the CMS
- (g) Data maintenance, retention, and disposition capabilities in accordance with Federal laws, standards, regulations, and guidelines, including the Privacy Act of 1974.
- (l) Secure transmission and receipt of applicant data to provide for integrity and confidentiality of data.
- (3) Business Process Management System: The Contractor shall have the capability to provide a business process management system , including all hardware and/or software, that shall provide the following functionalities:
- (a) Facilitates in maintenance of card holder lifecycle information

- (b) Manage submission of affiliation, adjudication and revocation data.
 - (c) Track progress of PIV applications through out process.
 - (d) Trace/audit PIV enrollments, particularly across different enrollment stations.
 - (e) Associate OPM suitability with PIV applicants directly.
 - (f) Manage associated processes like re-issuance, revocation, appeal.
 - (g) Provides access to multiple databases (i.e., IDMS, CMS).
 - (h) Manages interfaces with other PIV system components and agency systems, such as the following:
 - (1) Accepts affiliation data from agency systems.
 - (2) Accepts enrollment data from enrollment stations and/or and transmits applicant information to the stations.
 - (3) Sends fingerprints to OPM services for criminal history checks
 - (4) Accepts adjudication results from agency adjudicators, including authorization to begin production
 - (5) Sends cardholder information to card printing stations.
 - (6) Accepts the CHUID used for each cardholder
 - (7) Sends signed objects to the card management and production system for card insertion
- (4) CMS/IDMS/Business Process Management System Standard Configuration System: The Contractor shall have the capability to provide standard hardware and software configurations as follows:
- (a) Hardware that is sufficient to support all software functions, including peripherals and enough ports to connect all of them simultaneously. It must be of sufficient quality to operate up to 24 x 7 hours.
 - (b) Systems with standard configuration (i.e., operating system, hardware, and software) to provide all of the required functions.
 - (c) Capability to control access only to authorized operators and system administrators based on PIV card authentication.
 - (d) Capability to receive and send all data and notifications to authorized individuals and other PIV system components and services via secure, authenticated transmissions to provide integrity and confidentiality of the data.
 - (e) Secure delivery of standard configured system in accordance with order entity requirements and in accordance with secure shipping and delivery

processes, including delivery tracking and confirmation, only to authorized locations and authorities.

- (f) Inventory control system.
- (g) Audit and logging of systems infrastructure transactions including individual accountability for applicable functions completed.

3.1.1.1 Technical Standards Compliance

All systems infrastructure products related to the PIV card for which compliance is required must comply with HSPD-12, Federal Information Processing Standard 201 (FIPS 201), applicable National Institute of Standards and Technology (NIST) Special Publications (SP) and/or GSA interoperability compliance requirements. For categories of systems infrastructure products that require GSA approval (see <http://fips201ep.cio.gov/index.php>), the Contractor shall deliver only solution components that have been certified by NIST and approved by GSA, as appropriate, when such components are commercially available.

Approved FIPS 201-compliant products relate to provision of products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. 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 201 Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform tests for interoperability.

The Contractor shall have the capability to provide documentary evidence of FIPS 201 and GSA interoperability approval, or a plan to ensure that all products are fully compliant, for those hardware and software products that require FIPS 201 and GSA interoperability compliance.

3.1.1.2 Interface and Interoperability Support

To support communications with authorized officials and users, the hardware and software shall, at a minimum, support World Wide Web (WWW) Internet network access and interfaces for telecommunications services. The products shall support other network access interfaces and/or protocols as agreed between the ordering activity and the Contractor.

The products shall have the capability to implement software and interfaces that provide digital signature, authentication, data integrity, and privacy of personal data at rest and during transmission.

The PIV interface specification to support interoperability between PIV components provided by other Contractors and/or ordering entities (i.e., agencies) is currently under development. The Contractor shall have the capability to implement and support the PIV interface specification, at the time the PIV interface specification is published and required for all Contractors under SIN 132-62.

3.1.1.3 Systems Infrastructure Software

The Contractor shall have the capability to provide systems infrastructure software that, at a minimum, provides the following:

- (1) "Programmable screens" for to support CMS and IDMS data input and output:
- (2) All software interfaces shall be Section 508 compliant.
- (3) Output the data in shall be compliance with the data model and PIV object identifier requirements specified in FIPS 201 and NIST SP 800-76.
- (4) Interface to and interoperate with scheduling tools utilized for enrollment/registration and activation/finalization of PIV cards.

3.1.1.4 Security Standards Compliance

The Contractor shall have the capability to comply with FIPS 201, Appendix B, PIV Validation, Certification, and Accreditation, requirements.

3.1.1.5 Hardware and Software Maintenance Support

The Contractor shall, at a minimum, have the capability to provide support for hardware replacements in the event of hardware component failure, updates, and/or maintenance as follows:

- (1) If there is a component failure, the Contractor shall have the capability to ship replacements via next day shipping to minimize server down-time.
- (2) The Contractor shall have sufficient spare equipment on hand.

The Contractor shall have the capability to provide for update and maintenance of the associated product software as required to support modifications, enhancements, and license maintenance fees.

3.1.1.6 Special Contract Requirements

The Contractor shall have the capability to comply with the special contract requirements specified in SIN 132-62.

3.1.1.7 Allowance for Technology Changes

The Contractor shall create and have the capability to provide a robust infrastructure with sufficient flexibility to incorporate appropriate evolving technology.

The Contractor shall be able to incorporate new algorithms, formats, technologies, mechanisms, and media after contract award, as appropriate and approved by Government. The Government

recognizes that technologies are rapidly evolving and advancing. The Government wishes PIV card services, features, etc. to remain up-to-date with commercial equivalents. Accordingly, the Government anticipates that services, features, etc., available under SIN 132-62 will be increased, enhanced, and upgraded as these improvements become available.

The Contractor shall provide the capability to continue compliance and re-approval with NIST and GSA requirements for those services and products that require approval, throughout system and product lifecycle and technology changes.

Contractor shall propose enhancements which reduce the Government's risk, meet new or changed Government needs, improve performance, or otherwise present a service advantage to the Government.

3.1.1.8 Contractor Personnel Training

The Contractor shall have the capability to provide employees with proper training, update briefings, and comprehensive user manuals detailing procedures for performing duties related to providing PIV services, HSPD-12, and FIPS 201. The Contractor shall have the capability to provide documentation of the competence of employees and their satisfactory performance of duties relating to provision of these services.

3.1.1.9 Administrative and Personnel Security

The Contractor shall have the capability to provide documentary evidence of PIV equivalent identity verification and background checks for employees providing system configuration (i.e., operating system, software, and peripheral installations and configuration) for standard configuration stations.

3.1.1.10 Deliverables

The Contractor shall have the capability to provide the deliverables as specified in Table, 3.1.1.10-1, Deliverables.

Table 3.1.1.10-1. Deliverables

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|------------|--|--------------------------|---------------------------|-------------------------|--|
| 1 | Systems infrastructure hardware and software products. | As required in requests. | As required in request. | As required in request. | As required in request. |
| 2 | Standard configuration infrastructure hardware and software systems. | As required in requests. | As required in request. | As required in request. | As required in request. |
| 3 | A record of the transaction audit data resulting from deployment of the hardware and software products. | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request. |
| 4 | Audit reports that provide data necessary to monitor, reconcile, and audit system processing and reconciliation. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 5 | Program management reports providing information used to manage the PIV services. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|--|---|---|---|---|
| 6 | System fraud and security reports that will assist in the detection of fraud and ensure system security. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 7 | Record of approval to provide HSPD-12 compliant services and products, as specified in FIPS 201, NIST Special Publications, and GSA interoperability requirements, or plan to obtain approval. | As required in qualification requirements response package. |
| 8 | Responses to requests for Government approval of technology changes (i.e., new algorithms, formats, technologies, mechanisms, and media) | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 9 | Provide assurance of the trustworthiness and competence of employees. | As required in qualification requirements response package. |
| 10 | Fraud protection procedures | As required in request | As required in request | As required in request | 60 calendar days from contract award |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|---|------------------------|--|------------------------|--|
| 11 | Report of detection of unauthorized intrusion or any evidence of waste, fraud, or abuse | As required in request | Electronically, mail, or facsimile | As required in request | Immediately |
| 12 | Technical meetings | As required in request | As required in request | As required in request | As required in request |
| 13 | Monthly reports | One | Electronic access, plus one paper copy | As required in request | Within 10 business days of the end of the month covered in the report. |

3.1.1.11 Hardware and Software Products Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the systems infrastructure hardware and software products qualification requirements specified in this document as follows:

- (1) Written responses to all qualification requirements with sufficient information and descriptions to demonstrate to the Government that the Contractor understands the requirement and that the Contractor can provide the capabilities as specified.
- (2) To the extent the Contractor has the capability to provide multiple products and/or services in the three categories of services and products (i.e., hardware/software products, deployment services, and managed services), the Contractor may provide a consolidated response.
- (3) Documentary evidence of NIST and GSA approval for those products that require FIPS 201 and interoperability approval or a plan to obtain NIST and GSA approval for those products that require FIPS 201 and GSA approval as specified in Section 3.1.1.1.
- (4) Documentary evidence of competence of employees as specified in Section 3.1.1.8 of this document.
- (5) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.1.9 of this document.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements for submission of responses to this Statement of Qualification Requirements.

3.1.2 Systems Infrastructure Deployment Services

The Contractor shall have the capability to provide PIV systems infrastructure deployment services to agency locations, whether the Contractor or the agency owns, operates, and manages the systems infrastructure hardware and software.

The Contractor shall have the capability to provide the following PIV deployment support functionalities:

- (1) Centralized configuration to complete initial configurations of hardware and software.
- (2) Capability to apply software changes in a centralized model, including testing and minimal on-site steps.
- (3) Comprehensive inventory control including provision of on-line access to authorized authorities and PIV system components.
- (4) Secure shipping, including tracking capabilities only to authorized locations and authorities.
- (5) Setup instructions for installation at government sites.
- (6) On-site installation support.
- (7) Systems infrastructure personnel services as may be required.

3.1.2.1 Systems Infrastructure Hardware and Software Compliance

The Contractor shall have the capability to provide standard configuration systems infrastructure hardware and software products as part of deployment services that comply with all requirements specified in Section 3.1.1 of this document as part of deployment services.

3.1.2.2 Training

The Contractor shall have the capability to provide systems infrastructure training to government personnel specifically as follows:

The Contractor shall have the capability to provide card management and production training to government personnel specifically as follows:

- (1) In-person training. The Contractor shall have the capability to provide in-person training for government personnel who are performing systems infrastructure functions. The Contractor shall have the capability to provide in-person training at government locations and at Contractor provided training facilities.
- (2) On-line training: The Contractor shall have the capability to provide computer based training for agency personnel who are performing systems infrastructure with the following functionalities:
 - (a) Capability to provide complete information on the systems infrastructure process.
 - (b) Capability to be available and tracked via one of the approved government on-line training sites.
 - (c) Capability to test the trainee's competence and understanding of the information.
- (3) On-line installation video: The Contractor shall have the capability to provide an on-line installation video that is made available via the Internet and on the desktop to provide on-site installation processes and typical troubleshooting steps, including a "quick-help guide" for agency personnel performing on-site installation and configuration of systems infrastructure hardware and software.

3.1.2.3 Customer Service Center

The Contractor shall have the capability to provide a customer service center to provide help desk and other support functionalities for agency systems infrastructure personnel and PIV applicants as follows:

- (1) The capability to provide the following services for ordering agencies:
 - (a) Services, features, and options.
 - (b) Troubleshooting and problem reporting.
 - (c) Billing questions and issues.
 - (d) Implementation of services.
- (2) The capability to provide a toll free number and on-line access for problem

reporting and troubleshooting.

- (3) The capability to provide customer service center usage and activity data.
- (4) The capability to be available 24 hours a day, 7 days per week.
- (5) The capability to provide voice mail to handle incoming calls received at times when assigned staff is unavailable.
- (6) The capability to provide on-line information and support (e.g., maintenance of a web site for posting Frequently Asked Questions (FAQs) and general information).
- (7) The capability to provide an e-mail address for communicating with the customer service center.
- (8) The capability to respond to e-mail messages received automatically with a prompt acknowledgement of receipt and respond to content within 30 minutes.
- (9) The capability to implement and maintain a system for receiving, recording, responding to, and reporting customer service problems within its own organization and to the government.
- (10) The capability to implement and maintain a system of records relating to customer requests for services and the services provided. For each such request, the Contractor shall record sufficient information in order for the Government to determine who requested assistance, when the request was submitted, what action was required and/or resolution of the issue, and when the issue was resolved. At a minimum, the Contractor shall record the following information for each customer service request:
 - (a) Date/time initially contacted.
 - (b) Method of contact (e.g., telephone, e-mail, etc.).
 - (c) Name of individual making the contact.
 - (d) Type of service requested or problem reported.
 - (e) Action taken.
 - (f) Date/time action completed.
 - (g) Name of person taking the action.
 - (h) Requirements for follow-up action (if any).
 - (i) Date/time report filed.
 - (j) Name of person filing report.

- (k) Capability for customer service records to be made available for Government review or quality assurance inspection upon request.

3.1.2.4 Special Contract Requirements

The Contractor shall have the capability to comply with the special contract requirements specified in SIN 132-62.

3.1.2.5 Availability of Services

All of the on-line services and products specified shall, at a minimum, be in operation and available for use during the required hours of operation, not less than 99.5 percent of the time calculated on a monthly basis.

3.1.2.6 Response Time for Services

The Contractor shall, at a minimum, have the capability to provide the specified services according to the response times set forth in Table 3.1.2.6-1. All response times shall be measured from the time the Contractor receives an initiation message in its inbound queue until the time the Contractor's response leaves its outbound queue (i.e., from the time a request message is received until the time the response message is transmitted to the requestor).

Table 3.1.2.6-1. Response Time Requirements

| Transaction/Process | Response Time | Constraints |
|--|----------------------|--|
| On-site technical assistance | 5 days | >= 95% of all transactions within response |
| Response to trouble call | 30 minutes | >= 95% of all transactions within response |
| Replacement of hardware/software due to component failures | Next day shipping | >= 95% of all transactions within response |

3.1.2.7 Scalability and Implementation Schedule

The Contractor shall have the capability to provide a robust infrastructure to provide scalability and performance to support the service requirements of the ordering activity applications and IAW with the requirements in this Statement of Qualification Requirements.

The Contractor shall have the capability to provide an implementation schedule and plan that provides the required functionalities.

3.1.2.8 Allowance for Technology Changes

The Contractor shall create and have the capability to provide a robust infrastructure with sufficient flexibility to incorporate appropriate evolving technology.

The Contractor shall be able to incorporate new algorithms, formats, technologies, mechanisms, and media after contract award, as appropriate and approved by Government. The Government recognizes that technologies are rapidly evolving and advancing. The Government wishes PIV services, features, etc. to remain up-to-date with commercial equivalents. Accordingly, the Government anticipates that services, features, etc., available under SIN 132-62 will be increased, enhanced, and upgraded as these improvements become available.

Contractor shall propose enhancements which reduce the Government's risk, meet new or changed Government needs, improve performance, or otherwise present a service advantage to the Government.

3.1.2.9 Past Performance

The Contractor shall have the capability to provide detailed descriptions of past performance and prior experience related to large-scale government and/or non-government similar implementations for the Contractor and any member of the Contractor's team (e.g., subcontractor, joint venture, etc.) responsible for providing an estimated 25% or more of the services and products provided under an awarded contract.

The Contractor shall have the capability to provide information related to past performance and prior experience for the Contractor's largest projects (considering dollar value) completed or ongoing with an end date for each selected project not more than two years prior to the release of this Statement of Qualification Requirements.

The Contractor shall have the capability to provide the following past performance and prior experience information related to the Contractor's selected projects:

- (1) Compliance with technical or functional specifications or requirements.
- (2) Technology refreshment.
- (3) Quality of services and products;
- (4) Adherence to schedules.

3.1.2.10 Contractor Personnel Training

The Contractor shall have the capability to provide employees with proper training, update briefings, and comprehensive user manuals detailing procedures for performing duties related to providing PIV services, HSPD-12, and FIPS 20. The Contractor shall have the capability to provide documentation of the competence of employees and their satisfactory performance of duties relating to provision of these services.

3.1.2.11 Administrative and Personnel Security

The Contractor shall have the capability to ensure the integrity of deployment service operations including all personnel involved in system administration, security administration, systems infrastructure operators, on-site installation, troubleshooting, and training, and system configuration (i.e., operating system, software, and peripheral installations and configuration), services. The Contractor shall have the capability to provide documentary evidence of PIV equivalent identity verification and background checks for employees providing managed service operations.

3.1.2.12 Deliverables

The Contractor shall have the capability to provide the deliverables as specified in Table, 3.1.2.12-1, Deliverables.

Table 3.1.2.12-1. Deliverables

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|--|--------------------------|-------------------------|-------------------------|--|
| 1 | Deployment services as specified. | As required in requests. | As required in request. | As required in request. | As required in request. |
| 2 | A record of the transaction audit data resulting from provision of deployment services. | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request. |
| 3 | Audit reports that provide data necessary to monitor, reconcile, and audit system processing and reconciliation. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|------------|--|---|---|---|---|
| 4 | Program management reports providing information used to manage the PIV services. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 5 | System performance reports that monitor the operation and performance of the PIV services. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 6 | System fraud and security reports that will assist in the detection of fraud and ensure system security. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 7 | Record of approval to provide HSPD-12 compliant services and products, as specified in FIPS 201, NIST Special Publications, and GSA interoperability requirements, or a plan to obtain approval. | As required in qualification requirements response package. |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|--|---|---|---|--|
| 8 | Responses to requests for Government approval of technology changes (i.e., new algorithms, formats, technologies, mechanisms, and media) | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 9 | Provide assurance of the trustworthiness and competence of employees. | As required in qualification requirements response package. |
| 10 | Fraud protection procedures | As required in request | As required in request | As required in request | 60 calendar days from contract award |
| 11 | Report of detection of unauthorized intrusion or any evidence of waste, fraud, or abuse | As required in request | Electronically, mail, or facsimile | As required in request | Immediately |
| 12 | Trouble reports status | As required in request for procedures | Electronically, mail, or facsimile | As required in request | Within 4 hours after first report, updated every 4 hours thereafter |
| 13 | Technical meetings | As required in request |
| 14 | Monthly reports | One | Electronic access, plus one paper copy | As required in request | Within 10 business days of the end of the month covered in the report. |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|---|---|---|---|---|
| 15. | Information related to past performance as specified. | As required in qualification requirements response package. |
| I6 | Implementation schedule and plan. | As required in request. |

3.1.2.13 Project Management Office

The Contractor shall have the capability to provide a Project Management Office (PMO) to oversee all facets of the deployment services, including tracking of all systems infrastructure server deployment status and locations.

3.1.2.14 Deployment Services Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the systems infrastructure deployment services qualification requirements specified in this document as follows:

- (1) Written responses to all qualification requirements with sufficient information and descriptions to demonstrate to the Government that the Contractor understands the requirement and that the Contractor can provide the capabilities as specified, specifically the following “core” requirements:
 - (a) All technical and functional requirements.
 - (b) Past performance and experience in implementation of similar and/or equivalent enterprise services.
- (2) To the extent the Contractor has the capability to provide multiple products and/or services in the three categories of services and products (i.e., hardware/software products, deployment services, and managed services), the Contractor may provide a consolidated response.
- (3) Documentary evidence of past performance as specified in Section 3.1.2.9 of this document.
- (4) Documentary evidence of NIST and GSA approval for those products that require FIPS 201 and interoperability approval or a plan to obtain NIST and GSA

approval for those products that require FIPS 201 and GSA approval, as specified in Section 3.1.1.1.

- (5) Documentary evidence of competence of employees as specified in Section 3.1.2.10 of this document.
- (6) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.2.11 of this document.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements for submission of responses to this Statement of Qualification Requirements.

3.1.3 Managed Systems Infrastructure Services

The Contractor shall have the capability to provide managed systems infrastructure services, where the Contractor owns, operates, and manages systems infrastructure services and products at agency locations or Contractor locations, including the following:

- (1) Ownership, operation, maintenance, and management of systems infrastructure hardware and software.
- (2) Provision of systems infrastructure personnel.

The Contractor shall have the capability to provide managed PIV systems infrastructure functions as specified in the following sections.

3.1.3.1 Systems Infrastructure Hardware and Software Compliance

Contractors providing managed systems infrastructure services shall provide systems infrastructure products only as part of managed services. The Contractor shall have the capability to provide systems infrastructure hardware and software that comply with all requirements specified in Section 3.1.1 of this Qualifications Requirements Document.

3.1.3.2 Systems Infrastructure Deployment Services Compliance

The Contractor shall have the capability to provide systems infrastructure deployment services as part of managed systems infrastructure services that comply with all requirements specified in Section 3.1.2 of this Qualifications Requirements Document.

The Contractor shall have the capability to deliver quantities of PIV compliant PIV cards, with standard configuration and applicant personalization IAW FIPS 201 via secure shipping and delivery processes, including delivery tracking and confirmation, only to authorized locations and authorities.

3.1.3.3 IDMS, CMS and Business Process Management Services Compliance

The Contractor shall have the capability to provide managed IDMS, CMS, and Business Process Management Systems that comply with the all requirements specified in Section 3.1.1 of this Qualifications Requirements Document.

3.1.3.4 PIV Lifecycle Management

The Contractor shall have the capability to provide PIV card lifecycle management services which shall track the status of a PIV card throughout its entire lifecycle, from receipt of the sponsor's request, personalization and printing, finalization, revocation, termination, and destruction phases.

- (1) The Contractor shall have the capability to ensure that the card lifecycle management system houses the card management database that shall include a database management module to support maintenance of card holder information and card history data. This system shall retain data related to all card holders and shall provide sufficient backup and redundancy to ensure the integrity and availability of the data. The card lifecycle management system shall be available 24 hours per day and seven (7) days per week to accept card status updates and shall be available for on-line functions for support t other authorized PIV system services and other normal business functions. This system shall be configured to provide commercially acceptable response and throughput times for all transactions.
- (2) The Contractor shall have the capability to be responsible for all aspects of operation, maintenance, upgrades, and modifications of the central card lifecycle management system and shall provide adequate staffing with appropriate training to perform the operations and maintenance functions.
- (3) The Contractor shall have the capability to provide a card lifecycle management system that meets all of the requirements as specified.

3.1.3.5 Revocation and Termination

PIV cards are associated with a specific PIV account that contains attributes, privileges and other information required by other system components. The Contractor shall have the capability to immediately disable and terminate the PIV account and revoke and terminate the associated PIV card at the time a request for revocation and termination is received from the card holder, the Sponsor, or other authorized individual or component of the system.

The Contractor shall have the capability to provide a revocation and termination process that ensures the PIV account and associated PIV card can no longer be used.

- (1) At a minimum, the PIV account and associated PIV card shall be revoked and terminated under the following circumstances:
 - (a) The PIV card has been compromised, lost, or stolen.

- (b) The authentication credentials on the PIV card have been compromised.
 - (c) An employee separates (voluntarily or involuntarily) from the Agency.
 - (d) An employee separates (voluntarily or involuntarily) from the Agency's contractor.
 - (e) A contractor changes positions and no longer needs access to the Agency's buildings or systems.
 - (f) A PIV card holder is determined to hold a fraudulent identity or the PIV card has been fraudulent used.
 - (g) A PIV card holder passes away.
- (2) The Contractor shall have the capability to ensure that revocation and termination process of a PIV account and associated PIV card provides the following:
- (a) Processing of the request for revocation and termination of a PIV card received from the card holder, Sponsor, Issuer, other authorized agency officials, and authorized system services.
 - (b) Notification to the card holder, Sponsor, Issuer, other authorized agency officials, and other system services.
 - (c) A process for collection of the PIV card from the card holder.
 - (d) A process for destruction of the revoked and terminated PIV card.
 - (e) Maintenance of status information related to the revocation and termination processes.
 - (f) Disposition of personal data IAW Federal laws, standards, regulations and guidelines.

The Contractor shall have the capability to provide for emergency revocation and termination when such requests are received from the card holder, the Sponsor, or other authorized individual or component of the system.

3.1.3.6 Renewal

The Contractor shall have the capability to provide PIV card renewal (within 45 days prior to PIV card expiration) IAW FIPS 201.

The Contractor shall have the capability to provide PIV card renewal that includes the following:

- (1) Notification to the card holder, Sponsor, Issuer, other authorized agency officials, and other authorized system services prior to expiration of the PIV card.

- (2) Receipt of authorization for renewal from the Sponsor or other authorized agency official.
- (3) Re-verification and validation of the card holder's identity from data maintained in other PIV system services
- (4) Process for receipt and update of information received from other the system components.
- (5) Process for updating information in other system services.
- (6) Collection and destruction of expired PIV card.
- (7) Data records and maintenance as specified.

The expiration date of the PIV card authentication certificate and the optional digital signature certificate cannot be later than the expiration date of the PIV card; hence, support for generation of a new PIV authentication key and certificate shall be provided. If the PIV Card supports the optional key management key, it may be imported to the new PIV Card.

3.1.3.7 Replacement

The Contractor shall have the capability to replace damaged or lost valid PIV cards IAW the FIPS 201. If the PIV card has been compromised, revoked, and or terminated, the PIV card shall be re-issued IAW FIPS 201 and this document.

3.1.3.8 Re-issuance

- (1) The Contractor shall have the capability to provide for PIV card re-issuance under the following circumstances:
 - (a) The PIV card has expired.
 - (b) The PIV card has been revoked and terminated.
- (2) The Contractor shall have the capability to provide processes for PIV card re-issuance including the following:
 - (a) Process receipt of authorization for re-issuance from the Sponsor or other authorized agency official or authorized system services.
 - (b) Re-verification and validation of the card holder's identity from data maintained in other system services.
 - (c) Process for receipt and update of information received from other the system services.
 - (d) Process for updating information in other system services.
 - (e) Collection and destruction of expired or revoked and terminated PIV card.

- (f) Data records and maintenance as specified.

If a PIV card has been revoked, terminated, or expired, the Contractor shall have the capability to re-issue a smart IAW all registration, enrollment, and issuance requirements specified in FIPS 201 and this document.

3.1.3.9 Card Lifecycle Management Interactions

The card lifecycle management system shall interact either directly or indirectly with other authorized PIV systems. The Contractor shall have the capability to design the CMS to interact and be intra-operable with all other components within the system provided by the Contractor in accordance with the applicable PIV interface specifications as specified in this document. These include direct and/or indirect interactions with enrollment and registration, activation and finalization, and PKI systems. The Contractor shall have the capability to provide read/write permissions to the data constrained to authorized officials (i.e., Sponsors, Issuers) and authorized systems.

The Contractor shall have the capability to design the CMS to support interaction with other authorized systems to enable interoperability with PIV card systems provided by other Contractors IAW specifications and protocols to be defined by the Government. The Contractor shall have the capability to provide read/write permissions to data constrained to authorized officials and systems.

The Contractor shall have the capability to provide interaction with systems outside the PIV card system as required to complete registration/enrollment and provide support for agency-specific access controls via agreed upon protocols. These systems outside the card lifecycle management system include the following:

- (1). OPM systems for employment information.
- (2). Physical Access Control Systems (PACS).
- (3). Logical Access Control Systems (LACS).

All interactions within and outside the card lifecycle management system shall be via secure mechanisms that provide integrity and privacy of the data at rest and in transit.

3.1.3.10 Audit, Logging, and Standard Reporting

The Contractor shall have the capability to ensure that the technologies and systems used to collect, validate, transmit, and store a PIV card applicant's information are in compliance with the PIV privacy policies, specifically in FIPS 201 for PIV cards, and allow for continuous auditing:

- (1) The Contractor shall have the capability ensure that all identity and access activity shall have an auditable trail that can support forensic and system management capabilities, with the minimum capability to:

- (a) Reconstruct the chain of trust for issuance and management.
 - (b) Reconstruct access events to a given logical and/or physical asset.
 - (c) Reconstruct access events by an individual card holder.
- (2) The Contractor shall have the capability to provide a flexible sorting and reporting capability that allows information to be presented in graphical format, filtered and sorted as necessary to present usage, operations, security, auditing, and management information.
- (3) The Contractor shall have the capability to provide the following four categories of reports:
- (a) Audit Reports that shall provide data necessary to monitor, reconcile, and audit system processing and reconciliation.
 - (b) Program Management Reports that shall provide information that will be used to manage the organization's PIV services.
 - (c) System Performance Reports that shall monitor the operation and performance of the PIV card services system.
 - (d) System Fraud and Security Reports that shall provide information that will assist in the detection of fraud and ensure system security. At a minimum, data provided in System Fraud and Security Reports shall include the following information:
 - 1 Attempts (by location) to log on to the system using invalid passwords.
 - 2 Cards reported lost or stolen.
 - 3 Disputed or erroneous transactions.

3.1.3.11 Technical Standards Compliance

All data output from the systems infrastructure hardware and software products shall be in compliance with the following standards and guidelines, specifically in compliance with the data model and PIV object identifier requirements specified in FIPS 201 and NIST SP 800-76:

For those HSPD-12 PIV hardware and software products requiring compliance, the Contractor shall have the capability to provide a plan to ensure that all products are fully compliant with the following standards and guidelines and any certifications included in those standards:

- (1) FIPS 201: Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, National Institute of Standards and Technology (NIST), March 2006.

- (2) SP 800-73: Special Publication 800-73, Interfaces for Personal Identity Verification, National Institute of Standards and Technology (NIST), April 2005
- (3) Employees and Contractors, Office of Management and Budget, M-05-24, DRAFT 5 August 2005.
- (4) NIST SP 800-79: Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, Publication No. 800-79, NIST, July 2005.
- (5) NIST SP 800-76, PIV Biometric Data Specification.
- (5) NIST SP 800-78, PIV Cryptographic Algorithms for and Key Sizes.
- (6) NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

All card systems infrastructure products related to the PIV card for which compliance is required must comply with HSPD-12, Federal Information Processing Standard 201 (FIPS 201), applicable National Institute of Standards and Technology (NIST) Special Publications (SP) and/or GSA interoperability compliance requirements. For categories of systems infrastructure products that require GSA approval (see <http://fips201ep.cio.gov/index.php>), the Contractor shall deliver only solution components that have been certified by NIST and approved by GSA, as appropriate, when such components are commercially available.

Approved FIPS 201-compliant products relate to provision of products that have demonstrated compliance through evaluation and testing programs established by NIST and GSA. 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 201 Evaluation Program to evaluate other products needed for agency implementation of HSPD-12 requirements where normative requirements are specified in FIPS 201 and to perform tests for interoperability.

3.1.3.12 Interface and Interoperability Support

To support communications with authorized officials and users, the hardware and software shall, at a minimum, support World Wide Web (WWW) Internet network access and interfaces for telecommunications services. The products shall support other network access interfaces and/or protocols as agreed between the ordering activity and the Contractor.

The products shall have the capability to implement software and interfaces that provide digital signature, authentication, data integrity, and privacy of personal data at rest and during transmission.

The Contractor shall have the capability to provide interface and protocols for communications to support intra-operability among PIV components provided by the Contractor and for

integrated solutions provided by the Contractor.

If the product and/or integrated solution interfaces to a PIV component (i.e., agency PACS, LACS, enrollment/registration system) provided by another Contractor or agency, the Contractor shall have the capability to implement the PIV interface specification specified by the Government.

The PIV interface specification to support interoperability between PIV components provided by other Contractors and/or ordering entities (i.e., agencies) is currently under development. The Contractor shall have the capability to implement and support the PIV interface specification, at the time the PIV interface specification is published and required for all Contractors under SIN 132-62.

3.1.3.13 Security C&A and Re-Accreditation

The Contractor shall provide documentation of successful completion of a security audit related to systems infrastructure services and products that was conducted by an independent, trusted third party. The security audit shall have been conducted on similar deployed government or non-government systems.

For managed services provided at agency locations, the Contractor shall have the capability to provide support for completion of C&A in accordance with Section B of FIPS 201.

3.1.3.13.1 Plan for Completion of Initial C&A

The Contractor shall have the capability to provide a plan for completion of security C&A and for obtaining management Authority to Operate (ATO) from a Federal Government Designated Approving Authority (DAA) as follows:

- (1) The Contractor shall plan for completion of security C&A as required for storing, transmitting, and/or processing government information in an information system and/or approved system components or products provided by the Contractor at the Contractor facilities, and
- (2) The Contractor shall plan for support of security C&A as required for storing, transmitting, and/or processing government information in an information system and/or approved system components or products provided by the Contractor at Federal government facilities.

The plan for completion of C&A shall address the following:

- (1) The Contractor shall plan for completion of C&A IAW with Office of Management and Budget Circular A-130, Appendix III; Federal Information Security Management Act (FISMA) 2002, NIST 800-79, agency security policies, procedures, and guidelines, and FIPS 201.

- (2) The Contractor shall plan to have a security compliance audit conducted by an approved, independent trusted third-party and provide documentation of the results of the audit. That audit shall be conducted pursuant to guidance provided in the American Institute of Certified Public Accountants' (AICPA's) Statement on Auditing Standards (SAS) Number 70, Reports on the Process of Transactions by the Service Organizations, WebTrust Certification, and/or other applicable and approved guidance. The focus of this review shall be to provide the Government with independent verification that the Contractor is performing IAW with the applicable standards, requirements, FIPS 201, GSA policies and procedures, and this Statement of Qualification Requirements.
- (3) The Contractor shall plan to submit a C&A package in accordance with NIST SP 800-37. Guide for the Security Certification and Accreditation of Federal Information Systems, and the GSA security certification and accreditation guidelines and policies.

Documentation of applicable compliance audit requirements in force and effect at the time of security C&A shall be obtained from GSA.

3.1.3.13.2 Periodic Review of Security Controls

Periodic independent audits and reviews and re-accreditation shall occur IAW the standards and requirements in full force and effect on March 1, 2006, or as subsequently revised.

3.1.3.14 Date/Time Stamp Synchronization

The Contractor shall have the capability to implement date/time stamps as required for audit and logging of transactions and data. The Contractor shall use Coordinated Universal Time (UTC) NIST as the reference time base. Contractor's time shall be synchronized within one second and granularity of time expressed shall be at least to the granularity of one minute.

3.1.3.15 Performance

The Contractor shall have the capability to meet, at a minimum, the performance standards as specified for the following:

- (1) Hours of operation.
- (2) Availability of services.
- (3) Response time for services.

3.1.3.15.1 Hours of Operation

The Contractor shall have the capability to operate the following on-line services 24 hours per

day, 7 days per week, including Federal holidays:

- (1) Application acceptance and renewal services.
- (2) Verification and validation services.
- (3) Immediate PIV card revocation services.
- (4) Problem reporting.
- (5) Change reporting.

All of the remaining services and products specified shall, at a minimum, be operated on the basis of a 5-day, 40-hour work week, Monday through Friday, except Federal holidays.

3.1.3.15.2 Availability of Services

All of the on-line services and products specified shall, at a minimum, be in operation and available for use during the required hours of operation, not less than 99.5 percent of the time calculated on a monthly basis.

3.1.3.15.3 Response Time for Services

The Contractor shall, at a minimum, have the capability to provide the specified services according to the response times set forth in Table 3.1.3.15.3-1. All response times shall be measured from the time the Contractor receives an initiation message in its inbound queue until the time the Contractor's response leaves its outbound queue (i.e., from the time a request message is received until the time the response message is transmitted to the requestor).

Table 3.1.3.15.3-1. Response Time Requirements

| Transaction/Process | Response | Constraints |
|--|-----------------------|--|
| Data transferred between authorized PIV components | 3 sec (T1 1.54 mb) | >= 95% of all transactions within response |
| Revocation Request message | 5 min. | >= 95% of all transactions within response |

3.1.3.16 Customer Service Center

The Contractor shall have the capability to provide a customer service center to provide help desk and other support functionalities to card holders and ordering activities.

3.1.3.16.1 Services for Ordering Activity Applications

The customer service center shall assist authorized representatives of participating ordering

activities as follows:

- (1) Services, features, and options.
- (2) Troubleshooting and problem reporting.
- (3) Billing questions and issues.
- (4) Implementation of services.

3.1.3.16.2 Card Holder Services

The Contractor shall have the capability to provide customer service functions to card holders that include the following:

- (1) A customer service center with a toll free number and on-line access for cardholder inquiries.
- (2) A customer service center that provides personalized responses to:
 - (a) Report of lost, stolen, damaged, or inoperative cards.
 - (b) Report of unauthorized card use or other breach of security.
 - (c) Report of an update in demographic data.
 - (d) Required support for PIV card applications and services.
 - (e) Requests for PIN “unblock.”

The Contractor shall have the capability to provide customer service center usage and activity data.

The Contractor shall have the capability to provide information to cardholders for obtaining assistance from the Government. The Contractor shall have the capability to forward problems and/or inquiries received that concern services provided by order entities directly to the Government for resolution with the card holder (e.g., problems with accessing information being provided by ordering entities, inquiries/problems of a general nature about the PIV card program, etc.).

3.1.3.16.3 Hours of Operation

The customer service center shall be available 24 hours a day, seven days per week.

3.1.3.16.4 Toll-free Telephone Service

The customer service center shall have the capability to provide toll-free telephone service.

Voice mail capabilities shall be provided for handling incoming calls received at times when assigned staff is unavailable.

3.1.3.16.5 On-line and E-Mail Services

The customer service center shall provide on-line information and support to all card holders (e.g., maintenance of a web site for posting Frequently Asked Questions (FAQs) and general information to help cardholders).

The customer service center shall provide an e-mail address for use by all card holders in communicating with the customer service center.

The customer service center shall respond to e-mail messages received automatically with a prompt acknowledgement of receipt and respond to content in a time consistent with industry practices.

3.1.3.16.6 Problem Identification and Resolution

The customer service center shall implement and maintain a system for receiving, recording, responding to, and reporting customer service problems within its own organization and to the Government.

3.1.3.16.7 Customer Service Records

The customer service center shall implement and maintain a system of records relating to customer requests for services and the services provided. For each such request, the Contractor shall record sufficient information in order for the Government to determine who requested assistance, when the request was submitted, what action was required and/or resolution of the issue, and when the issue was resolved. At a minimum, the Contractor shall record the following information for each customer service request:

- (1) Date/time initially contacted.
- (2) Method of contact (e.g., telephone, e-mail, etc.).
- (3) Name of individual making the contact.
- (4) Individual agency application (if applicable).
- (5) Type of service requested or problem reported.
- (6) Action taken.
- (7) Date/time action completed.
- (8) Name of person taking the action.
- (9) Requirements for follow-up action (if any).
- (10) Date/time report filed.
- (11) Name of person filing report.

The Contractor shall provide the capability for customer service records to be made available for Government review or quality assurance inspection upon request.

3.1.3.17 Privacy Act Requirements

The Contractor will be maintaining one or more “systems of records” requiring protection under Section 552a, Title 5 of United States Code (5 U.S.C. 552a). The minimum standards for protecting and reporting on these systems of records are also set forth in 5 U.S.C. 552a. The regulations for protecting and reporting on these systems of records are set forth in Appendix I (Federal Agency Responsibilities for Maintaining Records About Individuals) to Office of Management and Budget (OMB) Circular Number A-130 (Management of Federal Information Resources).

Subsection (m) (1) of 5 U.S.C, 552a and Paragraph 3.a.(1) of Appendix I to OMB Circular Number A-130 provide that the systems of records protection and reporting requirements shall be passed through to any Contractor who maintains a system(s) of records on behalf of a Government agency.

The Contractor shall have the capability to meet the minimum systems of records protection and reporting requirements for the Contractor set forth in this Statement of Qualification Requirements.

3.1.3.18 Contractor Personnel Training

The Contractor shall have the capability to provide employees with proper training, update briefings, and comprehensive user manuals detailing procedures for performing duties related to providing PIV card services, HSPD-12, and FIPS 201. The Contractor shall have the capability to provide documentation of the competence of employees and their satisfactory performance of duties relating to provision of these services.

3.1.3.19 Data Transfer

The Contractor shall have the capability to initiate a complete transfer of all current and archived PIV card management data, policies and practices, billing, and audit data within 24 hours of request, or as otherwise agreed upon, IAW this Statement of Qualification Requirements, SIN 132-62, and according to Government-approved Data Transfer Plan. The Contractor shall maintain and keep up to date the Data Transfer Plan that is submitted as part of this Statement of Qualification Requirements. The data transferred shall not include any non-HSPD-12 services or non-government data.

3.1.3.20 Security/Privacy Requirements

3.1.3.20.1 Administrative and Personnel Security

The Contractor shall have the capability to ensure the integrity of managed service operations including all personnel involved in system administration, security administration, systems infrastructure operators, on-site installation, troubleshooting, and training, and system configuration (i.e., operating system, software, and peripheral installations and configuration) services. The Contractor shall have the capability to provide documentary evidence of PIV equivalent identity verification and background checks for employees providing managed service operations.

The Contractor shall have the capability to enforce the principle of separation of duties to ensure that no single individual has the capability to issue a smart card without the participation of another authorized person. The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.

3.1.3.20.2 Privacy Requirements

Unless otherwise specified, the data on the PIV card shall be limited to Sensitive but Unclassified data. While not subject to the regulations protecting classified data, nevertheless, such data shall be subject to privacy protection IAW the Privacy Act of 1974.

3.1.3.20.3 Data Retention

The Contractor shall have the capability to retain and archive all HSPD-12 PIV data in accordance with Federal data retention laws and regulations as specified by the U.S. National Archives and Records Administration.

3.1.3.21 Past Performance

The Contractor shall have the capability to provide detailed descriptions of past performance and prior experience related to large-scale government and/or non-government similar implementations for the Contractor and any member of the Contractor's team (e.g., subcontractor, joint venture, etc.) responsible for providing an estimated 25% or more of the services and products provided under an awarded contract.

The Contractor shall have the capability to provide information related to past performance and prior experience for the Contractor's largest projects (considering dollar value) completed or ongoing with an end date for each selected project not more than two years prior to the release of this Statement of Qualification Requirements.

The Contractor shall have the capability to provide the following past performance and prior experience information related to the Contractor's selected projects:

- (1) Compliance with technical or functional specifications or requirements.
- (2) Technology refreshment.
- (3) Quality of services and products;
- (4) Adherence to schedules.

3.1.3.22 Deliverables

The Contractor shall have the capability to provide the following deliverables as listed in Table 3.1.3.22-1, Deliverables.

Table 3.1.3.22-1. Deliverables

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|------------|--|--------------------------|---------------------------|-------------------------|--|
| 1. | Create and maintain such records as required for all data captured, stored, and maintained for each applicant. | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request. |
| 2. | Create and maintain such records as required for each applicant's and card holder's identity information. | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request. |
| 3. | A record of the transaction audit data resulting from deployment of the identity information to other system components and receipt of information from other system components. | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request. |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|---|--------------------------|-------------------------|-------------------------|--|
| 4. | A record of the transaction audit data resulting from PIV card life cycle management, including issuance, re-issuance, replacement, renewal, revocation, and termination. | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request. |
| 5. | Audit reports that provide data necessary to monitor, reconcile, and audit system processing and reconciliation. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 6. | Program management reports providing information used to manage the PIV services. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 7. | System performance reports that monitor the operation and performance of the PIV services. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 8. | System fraud and security reports that will assist in the detection of fraud and ensure system security. | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|--|---|---|---|---|
| 9. | Record of approval to provide HSPD-12 compliant services and products, as specified in FIPS 201, NIST Special Publications, and GSA interoperability requirements, or plan to obtain approval. | As required in qualification requirements response package. |
| 10. | Security audit, or Certification and Accreditation (C&A) and Re-Accreditation documentation as specified in NIST Special Publications, or C&A plan. | As required in qualification requirements response package. |
| 11. | Responses to requests for Government approval of technology changes (i.e., new algorithms, formats, technologies, mechanisms, and media) | As required in requests. | As required in request. | As required in request. | Within 30 calendar days of receipt of request. |
| 12. | A record of transaction audit data for each request received by the Customer Service Center | As required in requests. | As required in request. | As required in request. | Within 48 hours of receipt of request |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|------------|---|---|---|---|--|
| 13. | Provide assurance of the trustworthiness and competence of employees. | As required in qualification requirements response package. |
| 14. | Data Transfer Plan | As required in request | As required in request | As required in request | Within 24 hours of receipt of request |
| 15. | Fraud protection procedures | As required in request | As required in request | As required in request | 60 calendar days from contract award |
| 16. | Report of detection of unauthorized intrusion or any evidence of waste, fraud, or abuse | As required in request | Electronically, mail, or facsimile | As required in request | Immediately |
| 17. | Trouble reports status | As required in request for procedures | Electronically, mail, or facsimile | As required in request | Within 4 hours after first report, updated every 4 hours thereafter |
| 18. | Technical meetings | As required in request |
| 19. | Monthly reports | One | Electronic access, plus one paper copy | As required in request | Within 10 business days of the end of the month covered in the report. |
| 20. | Data collection forms | As required in request |

| No. | Descriptions of Deliverables | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|--|---|---|---|---|
| 21. | Request to establish a new or make a significant change to an existing systems of record reporting | As required in request | As required in request | As required in request | Not less than 60 working days prior to the requested implementation date. |
| 22. | Information related to past performance as specified. | As required in qualification requirements response package. |
| 12. | Implementation plan and schedule. | As required in request |

3.1.3.23 Project Management Office

The Contractor shall have the capability to provide a Project Management Office (PMO) to oversee all facets of the managed systems infrastructure services.

3.1.3.24 Systems Infrastructure Services Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the systems infrastructure managed services qualification requirements specified in this document as follows:

- (1) Written responses to all qualification requirements with sufficient information and descriptions to demonstrate to the Government that the Contractor understands the requirement and that the Contractor can provide the capabilities as specified, specifically in the following “core” requirements.
 - (a) All technical and functional requirements.
 - (b) Past performance and experience in implementation of similar and/or equivalent enterprise services.
 - (c) Documentary evidence (i.e., attestations) of a security assessment conducted by an independent, trusted third party, for a similar and/or equivalent enterprise implementation in accordance with Federal, international, or industry standard.
- (2) To the extent the Contractor has the capability to provide multiple products and/or services in the three categories of services and products (i.e., hardware/software products, deployment services, and managed services); the Contractor may provide a consolidated response.

- (3) Documentary evidence of past performance as specified in Section 3.1.3.21 of this document.
- (4) Documentary evidence of NIST and GSA approval for those products that require FIPS 201 and interoperability approval or a plan to obtain NIST and GSA approval for those products that require FIPS 201 and GSA approval, as specified in Section 3.1.3.11..
- (5) Documentary evidence of competence of employees as specified in Section 3.1.3.18 of this document.
- (6) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.3.20.1 of this document.
- (7) Documentary evidence of security audit, C&A, or plan for C&A, as specified in Section 3.1.3.13.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements for submission of responses to this Statement of Qualification Requirements.

3.2 Pricing

The Contractor shall have the capability to comply with the pricing requirements specified in SIN 132-62 and as specified in the following sections.

- (1) Pricing for systems infrastructure workstations shall not include the costs for the physical space. Physical space at agency locations for systems infrastructure servers will be provided by the Government.
- (2) All prices shall include all Contractor program management and administrative costs.
- (3) Hardware pricing shall include hardware replacements during the first five (5) years.
- (4) Software pricing shall include an annual maintenance price for updating with operating system patches and other software upgrades.

Appendix A: Qualification Requirements Submission Criteria

All information related to package submission in response to PIV Statements of Qualification Requirements is available at the GSA Identity Management web site: (www.idmanagement.gov), including statements of qualification requirements for all PIV services and products, application forms, submission instructions, and evaluation processes and procedures.

Contractors may submit requests for review of their qualifications in response to services and products in one or more of the following categories in this Statement of Qualification Requirements:

- (1) Systems infrastructure hardware and software products.
- (2) Systems infrastructure deployment services.
- (3) Managed systems infrastructure services.

Contractors may also submit requests for review of their qualifications in response to one or more Statements of Qualification Requirements for other SIN 132-62 HSPD-12 services and products.

A.1 General Instructions

- (1) The Contractor shall accurately complete the application cover sheet and submission package for the PIV services and products for which the Contractor is requesting review and approval.
- (2) The Contractor shall provide evidence and deliverables necessary to enable the Government to determine compliance with applicable approval criteria.
- (3) The Contractor shall provide technical staff, if needed, either onsite or via telephone, during the evaluation of the application and submission package.

A.2 Qualification Requirements Submission Contents

The contents of all submission packages in response to this Statement of Qualification Requirements shall be presented in three (3) sections as follows:

- (1) Section 1- Technical: Section 1 shall include responses to all functional and technical requirements as specified for each category of services and/or products for which the Contractor is requesting evaluation.
- (2) Section 2 – Past Performance: Section 2 shall include responses to all past performance requirements as specified for each category of services and/or products for which the Contractor is requesting evaluation.
- (3) Section 3 – Security: Section 3 shall include responses to all security requirements as specified for each category of services and products for which the Contractor is requesting evaluation.

A.3 Consolidated Responses

To the extent the Contractor is submitting responses to multiple categories of services and/or products specified in this Statement of Qualification Requirements, the Contractor may provide a consolidated response.

To the extent the Contractor is submitting responses to multiple Statements of Qualification Requirements for PIV services and products, the Contractor may provide a consolidated response for the following:

- (1) Section 2 – Past Performance. Section 2 shall include a consolidated response to all past performance requirements, including documentary evidenced, as specified for all PIV services and products included in the Contractor's submission package.
- (2) Section 3 – Security: Section 3 shall include a consolidated response to all security requirements, including documentary evidence, as specified for all PIV services and products included in the Contractor's submission package.
- (3) Documentary evidence related to the competence, integrity, and trustworthiness of employees.
- (4) Documentary evidence of plan for technical standards compliance.

A.4 Compliance Matrix

The Contractor shall submit a completed Systems Infrastructure Services and Products Compliance Matrix as part of their response to the Statement of Qualification Requirements for PIV services and products.

Systems Infrastructure Services and Products August 30, 2006 Compliance Matrix

| |
|--------------|
| Company Name |
|--------------|

| | |
|--------------------------|---------------------|
| <input type="checkbox"/> | Products |
| <input type="checkbox"/> | Deployment Services |
| <input type="checkbox"/> | Managed Services |

| |
|----------------------|
| Service/Product Name |
| |

Is this part of a consolidated response: **Yes** **No**
If Yes – indicate related services and products qualification requirements:

| | |
|--------------------------|-----------------------------|
| <input type="checkbox"/> | Integration Services |
| <input type="checkbox"/> | Activation and Finalization |

| | |
|--------------------------|-----------------------------|
| <input type="checkbox"/> | Enrollment and Registration |
| <input type="checkbox"/> | Card Production |

TECHNICAL REQUIREMENTS:

Systems Infrastructure Services – specific requirements – Section 3.1.1

NOTE: Provision of integration services requires integration of more than one HSPD-12 service and product.

Compliance Statement should be Concise: “We fully comply” or “We do not fully comply at this time.” You need only fill out the areas applicable to what you are applying for. Some areas are required for all three categories of services: “Hardware and Software Products,” “Deployment Services,” and “Managed Services.”

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 51. | Systems Infrastructure Software - required for all 3 categories <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.1.3 | |
| 52. | Hardware and Software Maintenance Support – required for all 3 categories <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.1.5 | |

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | | | |
| 53. | Deliverables Supporting Proposal Section: | 3.1.1.10 | |

Systems Infrastructure Deployment Services – specific requirements – Section 3.1.2

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 54. | Systems Infrastructure Hardware and Software Products Compliance Supporting Proposal Section: | 3.1.2.1 | |
| 55. | Training - – required for deployment and managed services Supporting Proposal Section: | 3.1.2.2 | |
| 56. | Customer Service Center – required deployment and managed services Supporting Proposal Section: | 3.1.2.3 3.1.3.16 | |
| 57. | Availability of Services – required for deployment and managed services Supporting Proposal Section: | 3.1.2.5 | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | | | |
| 58. | Response Time for Services Supporting Proposal Section: | 3.1.2.6 | |
| 59. | Scalability and Implementation Schedule – required for deployment and managed services Supporting Proposal Section: | 3.1.2.7 | |
| 60. | Project Management Office – required for deployment and managed services Supporting Proposal Section: | 3.1.2.13 3.1.3.19 | |
| 61. | Deliverables Supporting Proposal Section: | 3.1.2.12 | |

Managed PIV Integrated Services – specific requirements - Section 3.1.3

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 62. | Systems Infrastructure Hardware and Software Compliance Supporting Proposal Section: | 3.1.3.1 | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| | | | |
| 63. | Systems Infrastructure Deployment Services Compliance <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.2 | |
| 64. | IDMS, CMS, and Business Process Management Services <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.3 | |
| 65. | PIV Lifecycle Management <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.4 | |
| 66. | Revocation and Termination <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.5 | |
| 67. | Renewal <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.6 | |
| 68. | Replacement <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.7 | |
| 69. | Re-Issuance <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.8 | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | | | |
| 70. | Card Lifecycle Management Interactions <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.9 | |
| 71. | Availability of Services – required for deployment and managed services <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.2.5 | |
| 72. | Scalability and Implementation Schedule – required for deployment and managed services <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.2.7 | |
| 73. | Training - – required for deployment and managed services <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.2.2 | |
| 74. | Audit, Logging, and Standard Reporting <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.10 | |
| 75. | Date/Time Stamp Synchronization <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.14 | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| 76. | Performance <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.15 | |
| 77. | Customer Service Center – required for deployment and managed services <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.2.3 3.1.3.16 | |
| 78. | Data Transfer <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.19 | |
| 79. | Project Management Office – required for deployment and managed services <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.23 | |
| 80. | Deliverables <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.3.22 | |

Qualification Requirements that are “Common” to all Integration Services and Products

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 81. | Security Certification and Accreditation (C&A) and Re-Accreditation – see Security Requirements Evaluation Form | | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 82. | Privacy Act Requirements – See Security Requirements Evaluation Form | | |
| 83. | Past Performance – See Past Performance Requirements Evaluation Form | | |
| 84. | Technical Standards Compliance <div data-bbox="277 636 1073 789" style="border: 1px solid black; padding: 5px;">Supporting Proposal Section:</div> | 3.1.1.1 3.1.3.11 | |
| 85. | Interface and Interoperability Support <div data-bbox="277 842 1073 995" style="border: 1px solid black; padding: 5px;">Supporting Proposal Section:</div> | 3.1.1.2 3.1.3.12 | |
| 86. | Allowance for Technology Changes <div data-bbox="277 1047 1073 1201" style="border: 1px solid black; padding: 5px;">Supporting Proposal Section:</div> | 3.1.1.7 3.1.2.8 | |
| 87. | Contractor Personnel Training <div data-bbox="277 1253 1073 1407" style="border: 1px solid black; padding: 5px;">Supporting Proposal Section:</div> | 3.1.1.8 3.1.2.10 3.1.3.18 | |
| 88. | Special Contract Requirements <div data-bbox="277 1459 1097 1608" style="border: 1px solid black; padding: 5px;">Supporting Proposal Section:</div> | 3.1.1.6 3.1.2.4 | |

PAST PERFORMANCE REQUIREMENTS:

Systems Infrastructure Hardware and Software Products

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| 89. | Past performance is not evaluated for Systems Infrastructure hardware and software products submissions. Supporting Proposal Section: | | |

SECURITY REQUIREMENTS:

Systems Infrastructure Hardware and Software Products

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 90. | Security standards requirements Supporting Proposal Section: | 3.1.1.4 | |

Systems Infrastructure Deployment Services

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 91. | Security standards requirements Supporting Proposal Section: | 3.1.1.4 | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|-------------|---|----------------------|
| | | | |

| |
|--|
| Managed Systems Infrastructure Services |
|--|

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 92. | Security standards requirements <div data-bbox="277 932 1097 1087" style="border: 1px solid black; padding: 5px;"> Supporting Proposal Section: </div> | 3.1.1.4 | |
| 93. | Security Certification and Accreditation (C&A) and Re-Accreditation <ul style="list-style-type: none"> • Documentation/attestation of previous security audit on a similar system. • Documentation of previous management Authority to Operate (ATO) on a similar system. • Plan for obtaining ATO | 3.1.3.13 | |
| 94. | Privacy Act Requirements <div data-bbox="277 1411 1097 1566" style="border: 1px solid black; padding: 5px;"> Supporting Proposal Section: </div> | 3.1.3.17 | |
| 95. | Administrative Personnel Security <div data-bbox="277 1627 1097 1782" style="border: 1px solid black; padding: 5px;"> Supporting Proposal Section: </div> | 3.1.1.9 3.1.2.11 | |
| 96. | Security/Privacy Requirements <ul style="list-style-type: none"> • Administrative Personnel Security | 3.1.3.20. | |

Systems Infrastructure Systems Infrastructure Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|-----------------|---|--|-----------------------------|
| | <ul style="list-style-type: none">• Privacy Requirements• Data Retention <div data-bbox="277 583 1097 732" style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | | |