

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) Card Activation
and Finalization Services and Products

Statement of Qualification Requirements

Date: June 19, 2006
Revised August 30, 2006

GSA

U.S. General Services Administration
Federal Acquisition Service (FAS)

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..... | 4 |
| 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 | 5 |
| 2.4 | PIV Card Activation and Finalization Services and Products | 5 |
| 2.5 | Physical Access Control Services and Products..... | 5 |
| 2.6 | Logical Access Control Services and Products | 5 |
| 2.7 | PIV System Integration Services and Products | 5 |
| 2.8 | Approved FIPS 201-Compliant Services and Products | 5 |
| 2.9 | Professional Services..... | 6 |
| 2.10 | PIV Associated Systems..... | 6 |
| 2.10.1 | Agency-Specific Identity Management System (IDMS)..... | 6 |
| 2.10.2 | Office of Personnel Management (OPM)/Federal Bureau of Investigation (FBI) | |
| | 6 | |
| 2.11 | PIV Roles | 6 |
| 2.12 | Conceptual Overview of PIV Components..... | 7 |
| 2.13 | PIV Card Activation and Finalization Components..... | 8 |
| 3.0 | PIV Card Activation and Finalization Services and Products Qualification | |
| | Requirements | 9 |
| 3.1 | Scope and Description of Qualification Requirements | 10 |
| 3.1.1 | Card Activation and Finalization Hardware and Software Products | 12 |
| 3.1.1.1 | Technical Standards Compliance..... | 14 |
| 3.1.1.2 | Interface and Interoperability Support..... | 14 |
| 3.1.1.3 | Card Activation and Finalization Software | 14 |
| 3.1.1.4 | Security Standards Compliance | 15 |
| 3.1.1.5 | Hardware and Software Maintenance Support | 15 |
| 3.1.1.6 | Special Contract Requirements..... | 15 |
| 3.1.1.7 | Allowance for Technology Changes..... | 15 |
| 3.1.1.8 | Contractor Personnel Training..... | 16 |
| 3.1.1.9 | Administrative and Personnel Security..... | 16 |
| 3.1.1.10 | Deliverables | 16 |
| 3.1.1.11 | Hardware and Software Products Qualification Requirements Response | |
| | Package Submission | 18 |
| 3.1.2 | Card Activation and Finalization Deployment Services | 19 |
| 3.1.2.1 | Card Activation and Finalization Hardware and Software Compliance..... | 19 |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| | | |
|--------------|---|-----------|
| 3.1.2.2 | Scheduling Tool | 21 |
| 3.1.2.2.1 | <i>Applicant Interface</i> | 21 |
| 3.1.2.2.2 | <i>Issuer Interface</i> | 22 |
| 3.1.2.2.3 | <i>Administrative Interface</i> | 23 |
| 3.1.2.3 | Training | 23 |
| 3.1.2.4 | Customer Service Center | 24 |
| 3.1.2.5 | Special Contract Requirements | 26 |
| 3.1.2.6 | Availability of Services | 26 |
| 3.1.2.7 | Response Time for Services | 26 |
| 3.1.2.8 | Scalability and Implementation Schedule | 26 |
| 3.1.2.9 | Allowance for Technology Changes | 26 |
| 3.1.2.10 | Past Performance | 27 |
| 3.1.2.11 | Contractor Personnel Training | 27 |
| 3.1.2.12 | Administrative and Personnel Security | 27 |
| 3.1.2.13 | Deliverables | 28 |
| 3.1.2.14 | Project Management Office | 30 |
| 3.1.2.15 | Deployment Services Qualification Requirements Response Package Submission | 30 |
| 3.1.3 | Managed Card Activation and Finalization Services | 31 |
| 3.1.3.1 | Verification of Applicant | 31 |
| 3.1.3.2 | Card Activation | 31 |
| 3.1.3.3 | Cryptographic Key Generation and Receipt of Certificate(s) | 32 |
| 3.1.3.3.1 | <i>Acknowledgement of Receipt</i> | 32 |
| 3.1.3.4 | Post Issuance Processes | 32 |
| 3.1.3.4.1 | <i>Card Activation and Finalization Interactions</i> | 33 |
| 3.1.3.5 | Card Renewal | 34 |
| 3.1.3.5.1 | <i>Card Renewal Interactions</i> | 34 |
| 3.1.3.6 | Card Replacement | 34 |
| 3.1.3.6.1 | <i>Card Replacement Interactions</i> | 35 |
| 3.1.3.7 | Card Re-issuance | 35 |
| 3.1.3.7.1 | <i>Card Re-Issuance Interactions</i> | 36 |
| 3.1.3.8 | Card Revocation and Termination | 36 |
| 3.1.3.8.1 | <i>Card Revocation and Termination Interactions</i> | 37 |
| 3.1.3.9 | Card Activation and Finalization Hardware and Software Compliance | 37 |
| 3.1.3.10 | Card Activation and Finalization Deployment Services Compliance | 37 |
| 3.1.3.11 | Audit, Logging, and Standard Reporting | 37 |
| 3.1.3.12 | Technical Standards Compliance | 38 |
| 3.1.3.13 | Interface and Interoperability Support | 39 |
| 3.1.3.14 | Security Certification and Accreditation (C&A) and Re-Accreditation | 40 |
| 3.1.3.14.1 | <i>Plan for Completion of Initial C&A</i> | 40 |
| 3.1.3.14.2 | <i>Periodic Review of Security Controls</i> | 41 |
| 3.1.3.15 | Date/Time Stamp Synchronization | 41 |
| 3.1.3.16 | Performance | 41 |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| | | |
|--|---|-----------|
| 3.1.3.16.1 | Hours of Operation..... | 42 |
| 3.1.3.16.2 | Availability of Services | 42 |
| 3.1.3.16.3 | Response Time for Services..... | 42 |
| 3.1.3.17 | Customer Service Center | 43 |
| 3.1.3.17.1 | Services for Ordering Activity Applications..... | 43 |
| 3.1.3.17.2 | Card Holder Services..... | 43 |
| 3.1.3.17.3 | Hours of Operation..... | 44 |
| 3.1.3.17.4 | Toll-free Telephone Service | 44 |
| 3.1.3.17.5 | On-line and E-Mail Services | 44 |
| 3.1.3.17.6 | Problem Identification and Resolution..... | 44 |
| 3.1.3.17.7 | Customer Service Records..... | 44 |
| 3.1.3.18 | Privacy Act Requirements | 45 |
| 3.1.3.19 | Contractor Personnel Training..... | 45 |
| 3.1.3.20 | Data Transfer | 46 |
| 3.1.3.21 | Security/Privacy Requirements..... | 46 |
| 3.1.3.21.1 | Administrative and Personnel Security..... | 46 |
| 3.1.3.21.2 | Privacy Requirements..... | 46 |
| 3.1.3.21.3 | Data Retention..... | 47 |
| 3.1.3.22 | Past Performance | 47 |
| 3.1.3.23 | Deliverables | 48 |
| 3.1.3.24 | Project Management Office | 51 |
| 3.1.3.25 | Managed Card Activation and Finalization Services Qualification Requirements Response Package Submission | 51 |
| 3.2 | Pricing | 53 |
| Appendix A: Qualification Requirements Submission Criteria..... | | 1 |

List of Tables

Table 3.1-1. List of Card Activation and Finalization Services and Products Qualification Requirements10
Table 3.1.1.10-1. Deliverables16
Table 3.1.2.7-1. Response Time Requirements26
Table 3.1.2.13-1. Deliverables28
Table 3.1.3.16.3-1. Response Time Requirements42
Table 3.1.3.23-1. Deliverables48

List of Figures

Figure 2.12-1. Conceptual Overview of PIV Components7
Figure 2.13-1. PIV Card Activation and Finalization Components8

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 Homeland Security Presidential Directive (HSPD-12) Personal Identity Verification (PIV) 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. Contractor will be called upon to provide HSPD-12 PIV compliant services and products under individual Task/Delivery Orders issued in accordance with FSC 70 SIN 132-60 (SIN 132-60), Access Certificates for Electronic Services (ACES) Program, SIN 132-61, PKI Shared Service Providers (PKI SSP) Program, and SIN 132-62, HSPD-12 Product and Service Components.

This Statement of Qualification Requirements establishes the qualification requirements for providing PIV Card Activation and Finalization 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 Services and products consist of hardware, software components and supporting services that provide for identity assurance.

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

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

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

- 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 Group 70, SIN 132-62 (SIN 132-62), provides the specification of minimum technical functions and capabilities related to the HSPD-12 PIV Card Activation and Finalization 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 Card Activation and Finalization Services and Products. HSPD-12 PIV Card Activation and Finalization 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 (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

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

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.

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.

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 registration and enrollment 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.

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. Enrollment and Registration 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 Identity management Systems (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 Identity Management System (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 Office of Personnel Management (OPM)/Federal Bureau of Investigation (FBI)

All PIV applicant background investigations will be conducted through the Office of Personnel Management (OPM). OPM will conduct the investigations and forward results to the appropriate agency and/or PIV system component. The Federal Bureau of Investigation (FBI) 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:

- (a) **Applicant** – The individual to whom a PIV credential needs to be issued.
- (b) **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.
- (c) **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.
- (d) **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.

- (e) **PIV Digital Signatory**—The entity that digitally signs the PIV biometrics and CHUID.
- (f) **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.

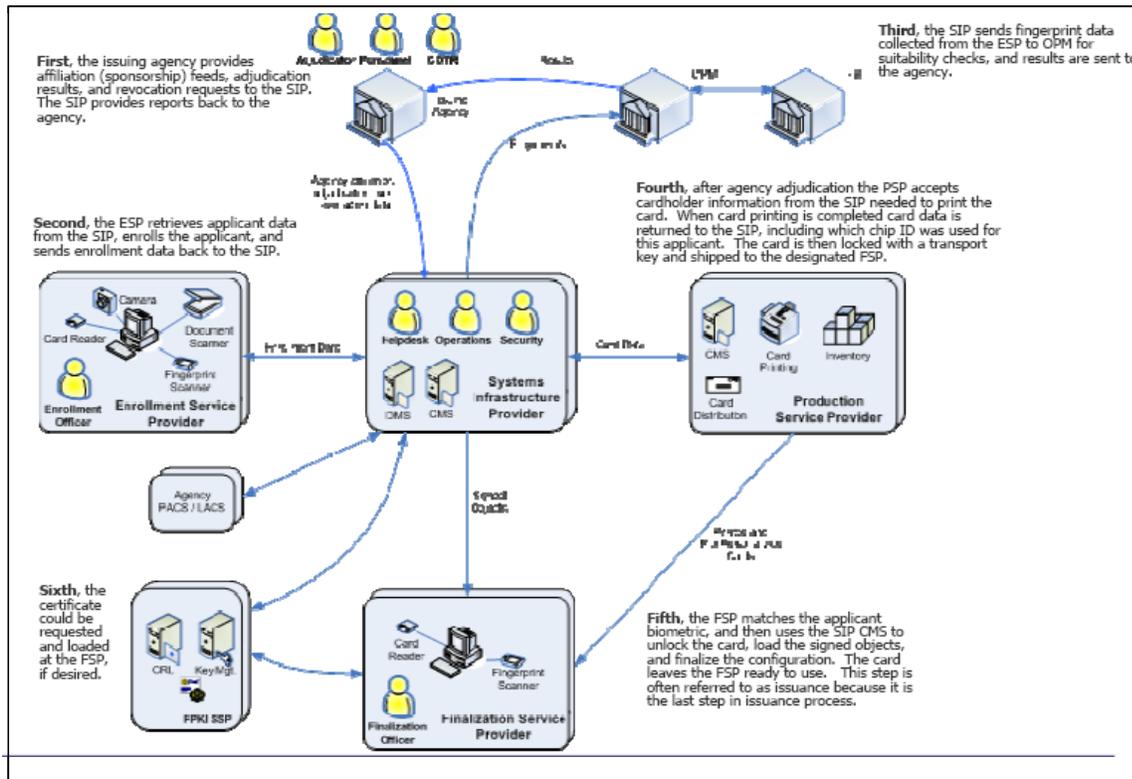


Figure 2.12-1. Conceptual Overview of PIV Components

2.13 PIV Card Activation and Finalization Components

Figure 2.13-1, PIV Card Activation and Finalization Components, depicts the components that incorporate the scope of the qualifications document.

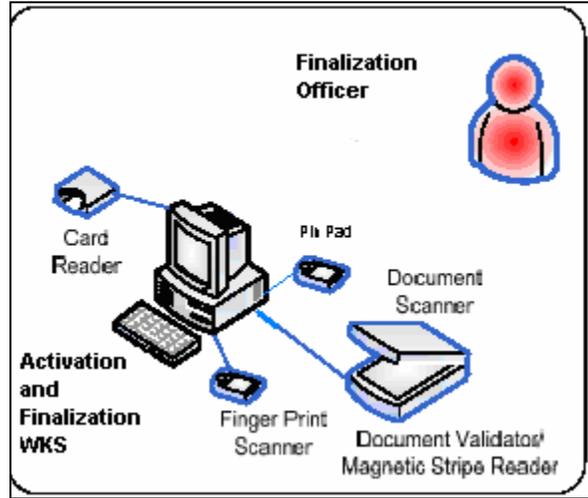


Figure 2.13-1. PIV Card Activation and Finalization Components

3.0 PIV Card Activation and Finalization Services and Products Qualification Requirements

This Statement of Qualification Requirements under FSC Group70, SIN 132-62 (SIN 132-62), provides the specification of minimum technical functions and capabilities related to the provision of HSPD-12 PIV Card Activation and Finalization 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 Card Activation and Finalization Services and Products.

The Contractor shall have the capability to provide card activation and finalization of PIV applicants. The Contractor shall have the capability to collect, store, and maintain all information and documentation required to verify and assure the applicant's identity related to card activation and finalization IAW FIPS 201. .

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

- (1) Card activation and finalization hardware and software products.
- (2) Card activation and finalization deployment services.
- (3) Managed card activation and finalization services.

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

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

All services and 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 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 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.

3.1 Scope and Description of Qualification Requirements

The scope and descriptions of the qualification requirements for provision of HSPD-12 PIV Card Activation and Finalization Services and Products are defined in the following sections. Table 3.1-1, List of Card Activation and Finalization 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 Card Activation and Finalization Services and Products Qualification Requirements

| Requirement No. | Description | Section References |
|--|---|---------------------------|
| Card Activation and Finalization Hardware and Software Products | | |
| 1. | Card Activation and Finalization Hardware and Software Products | 3.1.1 |
| 2. | Technical Standards Compliance | 3.1.1.1 |
| 3. | Interface and Interoperability Support | 3.1.1.2 |
| 4. | Card Activation and Finalization Software | 3.1.1.3 |
| 5. | Security Standards Compliance | 3.1.1.4 |
| 6. | Hardware and Software Maintenance Support | 3.1.1.5 |
| 7. | Special Contract Requirements | 3.1.1.6 |
| 8. | Allowance for Technology Changes | 3.1.1.7 |
| 9. | Contractor personnel Training | 3.1.1.8 |
| 10. | Administrative Personnel Security | 3.1.1.9 |
| 11. | Deliverables | 3.1.1.10 |
| 12. | Response Package Submission | 3.1.1.11 |
| Card Activation and Finalization Deployment Services | | |
| 13. | Card Activation and Finalization Hardware and Software Compliance | 3.1.2.1 |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Requirement No. | Description | Section References |
|--|---|---------------------------|
| 14. | Scheduling Tool | 3.1.2.2 |
| 15. | Training | 3.1.2.3 |
| 16. | Customer Service Center | 3.1.2.4 |
| 17. | Special Contract Requirements | 3.1.2.5 |
| 18. | Availability of Services | 3.1.2.6 |
| 19. | Response Time for Services | 3.1.2.7 |
| 20. | Scalability and Implementation Schedule | 3.1.2.8 |
| 21. | Allowance for Technology Changes | 3.1.2.9 |
| 22. | Past Performance | 3.1.2.10 |
| 23. | Contractor Personnel Training | 3.1.2.11 |
| 24. | Administrative and Personnel Security | 3.1.2.12 |
| 25. | Deliverables | 3.1.2.13 |
| 26. | Project Management Office | 3.1.2.14 |
| 27. | Response Package Submission | 3.1.2.15 |
| Managed Card Activation and Finalization Services | | |
| 28. | Verification of Applicant | 3.1.3.1 |
| 29. | Card Activation | 3.1.3.2 |
| 30. | Cryptographic Key Generation and Receipt of Certificate(s) | 3.1.3.3 |
| 31. | Post Issuance Processes | 3.1.3.4 |
| 32. | Card Renewal | 3.1.3.5 |
| 33. | Card Replacement | 3.1.3.6 |
| 34. | Card Re-Issuance | 3.1.3.7 |
| 35. | Card Revocation and Termination | 3.1.3.8 |
| 36. | Card Activation and Finalization Hardware and Software Compliance | 3.1.3.9 |
| 37. | Card Activation and Finalization Deployment Services | 3.1.3.10 |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Requirement No. | Description | Section References |
|------------------------|---|---------------------------|
| | Compliance | |
| 38. | Audit, Logging, and Standard Reporting | 3.1.3.11 |
| 39. | Technical Standards Compliance | 3.1.3.12 |
| 40. | Interface and Interoperability Support | 3.1.3.13 |
| 41. | Security Certification and Accreditation (C&A) and Re-Accreditation | 3.1.3.14 |
| 42. | Date/Time Stamp Synchronization | 3.1.3.15 |
| 43. | Performance | 3.1.3.16 |
| 44. | Customer Service Center | 3.1.3.17 |
| 45. | Privacy Act Requirements | 3.1.3.18 |
| 46. | Contractor Personnel Training | 3.1.3.19 |
| 47. | Data Transfer | 3.1.3.20 |
| 48. | Security/Privacy Requirements | 3.1.3.21 |
| 49. | Past Performance | 3.1.3.22 |
| 50. | Deliverables | 3.1.3.23 |
| 51. | Project Management Office | 3.1.3.24 |
| 52. | Response Package Submission | 3.1.3.25 |
| Pricing | | |
| 53. | Pricing | 3.2 |

3.1.1 Card Activation and Finalization Hardware and Software Products

The Contractor shall have the capability to provide card activation and finalization 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 card activation and finalization information:

- (1) Personal computer: The computer must meet all of the specifications of the included peripherals and have enough ports to connect all of them simultaneously. At a minimum, the computer must meet the following standards.

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

- (a) Pentium IV
 - (b) 1 GHZ CPU
 - (c) Windows XP Pro
 - (d) 1 GB RAM
 - (e) DVD Drive
 - (f) 40GB internal disk drive
 - (g) Sufficient USB2 ports to connect all USB2 supported components
 - (h) Sufficient Firewire ports to connect all Firewire supported components
 - (i) Sufficient RS232 ports to connect all components
- (2) PIV Card Reader: The Contractor shall have the capability to provide FIPS 201 and GSA approved products.
- (a) Fingerprint Reader: The Contractor shall have the capability to provide FIPS 201 and GSA approved products.
- (3) Personal Identification Number (PIN) pad.
- (4) Ancillary Parts: Ancillary parts and/or hardware shall, at a minimum, provide the following:
- (a) Optical mouse.
 - (b) Power cords and all connector cables.
 - (c) Surge protectors.
- (5) Supplies: The Contractor shall have the capability to provide the supplies for each card activation and finalization station (i.e., protective film for scanner).
- (6) The Contractor shall have the capability to provide standard configuration hardware and software stations 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 transactions including individual accountability for applicable functions completed.

3.1.1.1 Technical Standards Compliance

All card activation and finalization 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 card activation and finalization 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 Card Activation and Finalization Software

The Contractor shall have the capability to provide card activation and finalization software that, at a minimum, provides the following:

- (1) “Programmable screens” for card activation and finalization data collection to support the following functionalities:
 - (a) Capture images for all identity documents.
 - (b) Capability to match documents to available templates and/or examine security features to ensure authenticity.
 - (c) Capability to be configured to reject some documents where the name does not perfectly match the name from the applicant’s record in the PIV system.
 - (d) Capability to capture biometric data.
 - (e) Capability for digital signature and submission of activation and finalization data.
- (2) All software interfaces for use by agency operators and end-users shall be Section 508 compliant.
- (3) Output the data in compliance with the data model and PIV object identifier requirements specified in FIPS 201 and NIST SP 800-76.

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 station 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 for 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.

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 2006

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 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.

3.1.1.9 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 Deliverable | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|---|--------------------------|-------------------------|-------------------------|-------------------------|
| 1 | Card activation and finalization approved hardware and software products. | As required in requests. | As required in request. | As required in request. | As required in request. |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| No. | Descriptions of Deliverable | Quantity | Medium of Delivery | Where to Deliver | Submittal Date |
|-----|--|---|---|---|---|
| 2 | Card activation and finalization standard configuration stations. | 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 distribution 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. |
| 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 Homeland Security Presidential Directive 12 (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. |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| No. | Descriptions of Deliverable | 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 | Technical meetings | As required in request |
| 13 | Monthly reports | One (1) | Electronic access, plus 1 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 card activation and finalization hardware and software products qualification requirements specified in this document as follows:

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 2006

- (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.
- (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 on submission of responses to this Statement of Qualification Requirements.

3.1.2 Card Activation and Finalization Deployment Services

The Contractor shall have the capability to provide PIV card activation and finalization deployment services at agency locations, whether the Contractor or the agency owns, operates, and manages the card activation and finalization 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) Card activation and finalization personnel services as may be required.

3.1.2.1 Card Activation and Finalization Hardware and Software Compliance

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 2006

The Contractor shall have the capability to provide card activation and finalization 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 Scheduling Tool

The Contractor shall have the capability to provide a web-based scheduling tool with the following functionalities:

- (1) Graphically look up and locate the card activation and finalization service assigned to an applicant.
- (2) Assistance in managing location and availability of a specific card activation and finalization station.
- (3) Assistance in managing availability of issuer(s) assigned to a card activation and finalization station.
- (4) Assistance in managing appointments of applicants by card activation and finalization station.
- (5) E-mail notification to issuers and/or applicants if schedules/locations change.

3.1.2.2.1 Applicant Interface

The Contractor shall have the capability to provide an applicant interface to the web-based scheduling tool that provides the following functionalities:

- (1) Web based, publicly accessible:
- (2) Automatic search functionality.
 - (a) User enters Registration ID number.
 - (b) Results returned to the user.
- (4) Locations with more than one station:
 - (a) Multiple stations in a single location should have only one calendar but allow multiple entries per time slot.
- (5) Search individual locations by time and date:
 - (a) Times should be displayed as available or not available.
- (6) Individuals should be assigned times by Registration ID number:
 - (a) Forgotten Registration IDs can be found by searching last name, date of birth, and last four digits of social security number.
- (7) Cancellation/ rescheduling of appointment time:
 - (a) Recall previous appointment time by looking up Registration ID.
 - (b) Make changes to date and/ or time of appointment.
 - (c) Change will automatically cancel previous time.

- (d) Only one reservation per person may be held at a time.
- (8) Data Elements required for Applicant Interface:
 - (a) Station Address.
 - (b) Station City.
 - (c) Station State.
 - (d) Station Zip.
 - (e) Station Agency Affiliation.
 - (f) Date (s).
 - (g) Time.
 - (h) Registration ID.
 - (i) Applicant Phone (optional).
 - (j) Applicant Email.
 - (k) Applicant Last Name.
 - (l) Applicant Date of Birth.
 - (m) Applicant Last Four Digits Social Security Number.

3.1.2.2.2 Issuer Interface

The Contractor shall have the capability to provide an issuer interface to the web-based scheduling tool that provides the following functionalities:

- (1) Web based – Protected from public.
- (2) Set station schedule and location information.
- (3) View Schedule.
- (4) Manual Appointment Changes/ Cancellations.
- (5) Audit trail of all changes.
- (6) Data Elements required for Issuer Interface:
 - (a) Station Building Name.
 - (b) Station Address.
 - (c) Station City.
 - (d) Station State.
 - (e) Station Zip.

- (f) Applicant Last Name.
- (g) Applicant Date of Birth.
- (h) Applicant Last Four Digits Social Security Number.
- (i) Date (s).
- (j) Time.
- (k) Registration ID.
- (l) Station Agency Affiliation.
- (m) Station Phone.
- (n) Station Email.
- (o) Special Instructions Field.

3.1.2.2.3 Administrative Interface

The Contractor shall have the capability to provide an administrative interface to the web-based scheduling tool that provides the following functionalities:

- (1) Administrative Interface shall have the same functionality as Issuer Interface for all stations.
- (2) Generate utilization reports (i.e., number of PIV cards issued).
- (3) Configure role assignments by station.
- (4) Add/remove station.
- (5) Data Elements required for Administrative Interface:
 - (a) Station Building Name.
 - (b) Station Address.
 - (c) Station City.
 - (d) Station State.
 - (e) Station Zip.
 - (f) Station Agency Affiliation.
 - (g) Station Phone.
 - (h) Station Email.
 - (i) Special Instructions Field.

3.1.2.3 Training

The Contractor shall have the capability to provide card activation and finalization 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 card activation and finalization of PIV applicants. 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 card activation and finalization of PIV applicants with the following functionalities:
 - (a) Capability to provide complete information on the card activation and finalization 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 card activation and finalization hardware and software.
- (4) On-line PIV applicant training: The Contractor shall have the capability to provide on-line information and training that is accessible via the Internet and available at the card activation and finalization site locations for all PIV applicants.

3.1.2.4 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 card activation and finalization 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.

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

- (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.

3.1.2.5 Special Contract Requirements

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

3.1.2.6 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.

3.1.2.7 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 3.1.2.7-1. 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 3.1.2.7-1. 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 min. | >= 95% of all transactions within response |
| Replacement of hardware/software due to component failures | Next day shipping | >= 95% of all transactions within response |

3.1.2.8 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.

3.1.2.9 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.

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.

3.1.2.10 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.

3.1.2.11 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.

3.1.2.12 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, card

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

activation and finalization 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.

3.1.2.13 Deliverables

The Contractor shall have the capability to provide the deliverables as specified in Table, 3.1.2.13-1, Deliverables.

Table 3.1.2.13-1. 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. |
| 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. |

Card Activation and Finalization 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 |
|-----|--|---|---|---|---|
| 7 | Record of approval to provide Homeland Security Presidential Directive 12 (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. |
| 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 |

Card Activation and Finalization 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 |
|-----|---|---|---|---|--|
| 14 | Monthly reports | One (1) | Electronic access, plus 1 paper copy | As required in request | Within 10 business days of the end of the month covered in the report. |
| 15 | Information related to past performance as specified. | As required in qualification requirements response package. |
| 16 | Implementation schedule and plan. | As required in request. | As required in request. | As required in request | As required in request. |

3.1.2.14 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 card activation and finalization station deployment status and locations.

3.1.2.15 Deployment Services Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the card activation and finalization 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 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.
- (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 3.1.2.10 of this document.

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 2006

- (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.
- (5) Documentary evidence of competence of employees as specified in Section 3.1.2.11 of this document.
- (6) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.2.12 of this document.

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

3.1.3 Managed Card Activation and Finalization Services

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

- (1) Ownership, operation, maintenance, and management of card activation and finalization hardware and software.
- (2) Provision of card activation and finalization personnel.

The Contractor shall have the capability to provide managed PIV card activation and finalization functions as specified in the following sections.

3.1.3.1 Verification of Applicant

The Contractor shall have the capability to provide support for the following verification of the applicant:

- (1) That the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.
- (2) That the applicant is registered in the card management data records system.
- (3) That the approval notification is consistent with the results of the background investigation.
- (4) That the card has been produced, personalized, and is on the premises.
- (5) That the fingerprint of the individual matches the biometric credential embedded in the PIV Card or the applicant's record in the IDMS.

The card activation and finalization services shall have the capability to retain all card activation and finalization data records.

3.1.3.2 Card Activation

The Contractor shall have the capability to provide support for card activation as follows:

- (1) Provision of the PIN by the applicant.
- (2) Generation of a PIN on behalf of the applicant to verify the PIN and the correct card operation.
- (3) Verification of the correct operation of the card.

3.1.3.3 Cryptographic Key Generation and Receipt of Certificate(s)

The Contractor shall have the capability to provide support for cryptographic key generation and receipt of Public Key Infrastructure (PKI) certificates as follows:

- (1) Generation of cryptograph key pair(s) by the applicant.
- (2) Capability to obtain PKI certificates from the PIV PKI Certificate Authority (CA).
- (3) Provision of a one-time authenticator for use by the applicant to obtain PKI certificates at another time and location.

3.1.3.3.1 Acknowledgement of Receipt

The Contractor shall provide the capability to provide support for obtaining an acknowledgement of receipt of the card as follows:

- (1) Obtain a signature from the applicant attesting to the applicant's receipt and acceptance of the card
- (2) Obtain a signature from the applicant acknowledging acceptance of related responsibilities for usage of the card and procedures for card loss, damage, and/or fraudulent use.

3.1.3.4 Post Issuance Processes

The Contractor shall have the capability to provide support for post-issuance processes following receipt by the applicant as follows:

- (1) Notification to the PIV Sponsor indicating successful completion of card activation and finalization.
- (2) Notification to the PIV Issuer indicating successful completion of card activation and finalization.
- (3) Notification to the PIV Sponsor indicating unsuccessful completion of card activation and finalization.
- (4) Notification to the PIV Issuer indicating unsuccessful completion of card activation and finalization.
- (5) Update card activation and finalization status information the card management data records system.

- (6) Maintenance of the following information:
 - (a) Completed and formally authorized PIV request.
 - (b) Approval notice from the PIV issuer.
 - (c) Name of applicant.
 - (d) Credential identifier (card serial number).
 - (e) Expiration date of the card.
 - (f) Signed acknowledgement of receipt by the applicant.

The card activation and finalization services shall have the capability to retain all card activation and finalization data records and be responsible for providing an applicant's data record to be used by the other PIV system components (i.e., infrastructure services). The card activation and finalization services shall have the capability to provide and transmit all data and information via secure means to protect the integrity and privacy of the data.

3.1.3.4.1 Card Activation and Finalization Interactions

The Contractor shall have the capability to interact with other PIV systems and services as follows:

- (1) Secure receipt of identity information from the system infrastructure.
- (2) Secure notification to authorized individuals and other authorized system components on the status of card activation and finalization.
- (3) Secure distribution of information to the system infrastructure.
- (4) Interaction with the card to verify its operation.
- (5) Interaction with the card to provide generation of key pairs(s) and receipt of PKI certificates
- (6) Interaction with the applicant for verification of identity and acknowledgement of receipt of the card and acceptance of the card usage rules.

3.1.3.5 Card Renewal

The Contractor shall have the capability to provide support for PIV card renewal IAW FIPS 201 and as follows.

- (1) Verification of authorization for renewal from the Sponsor or other authorized agency official.
- (2) Re-verification and validation of the card holder's identity from data maintained in other PIV system services
- (3) Process for updating card renewal information in other system services.
- (4) Verification of operation of the card, including card activation, cryptographic key generation and receipt of PKI certificates.
- (5) Collection and destruction of expired PIV card.
- (6) Data records and maintenance as specified.

3.1.3.5.1 Card Renewal Interactions

The Contractor shall have the capability to interact with other PIV systems and services as follows:

- (1) Secure receipt of request for renewal and information updates from the applicant, Sponsor, and other PIV system components.
- (2) Secure verification of authorization from the Sponsor.
- (3) Secure distribution of information to other PIV system components.
- (4) Secure receipt of information from other PIV system components.
- (5) Secure notification to authorized individuals and other authorized system components on the status of the card renewal.
- (6) Interact with the PIV card to verify its operation.
- (7) Interact with the applicant for verification of identity and acknowledgement of receipt of the renewed PIV card.

3.1.3.6 Card Replacement

The Contractor shall have the capability to provide replacement of 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 as follows:

- (1) Verification of authorization for renewal from the Sponsor or other authorized agency official.
- (2) Re-verification and validation of the card holder's identity from data maintained in other PIV system services
- (3) Process for updating card renewal information in other system services.
- (4) Verification of operation of the card, including card activation, cryptographic key generation and receipt of PKI certificates.
- (5) Collection and destruction of expired PIV card.

- (6) Data records and maintenance as specified.

3.1.3.6.1 Card Replacement Interactions

The Contractor shall have the capability to interact with other PIV systems and services as follows:

- (1) Secure receipt of request for replacement and information updates from the applicant, Sponsor, and other PIV system components.
- (2) Secure verification of authorization from the Sponsor.
- (3) Secure distribution of information to other PIV system components.
- (4) Secure receipt of information from other PIV system components.
- (5) Secure notification to authorized individuals and other authorized system components on the status of the card replacement.
- (6) Interaction with the PIV card to verify its operation.
- (7) Interaction with the applicant for verification of identity and acknowledgement of receipt of the renewed PIV card.

3.1.3.7 Card Re-issuance

The Contractor shall have the capability to provide for PIV card re-issuance under the following circumstances:

- (1) The PIV card has expired.
- (2) The PIV card has been revoked and terminated.

The Contractor shall have the capability to provide processes for PIV card re-issuance, including the following:

- (1) Process receipt of authorization for re-issuance from the Sponsor or other authorized agency official or authorized system services.
- (2) Re-verification and validation of the card holder's identity from data maintained in other system services.
- (3) Process for receipt and update of information received from other the system services.
- (4) Verification of operation of the card, including card activation, cryptographic key generation and receipt of PKI certificates.
- (5) Process for updating information in other system services.
- (6) Collection and destruction of expired or revoked and terminated PIV card.
- (7) 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 issuance requirements specified in FIPS 201 and this Statement of Qualification Requirements.

3.1.3.7.1 Card Re-Issuance Interactions

- (1) Secure receipt of request for re-issuance and information updates from the applicant, Sponsor, and other PIV system components.
- (2) Secure receipt of authorization from the Sponsor.
- (3) Secure distribution of information to other PIV system components.
- (4) Secure receipt of information from other PIV system components.
- (5) Secure notification to authorized individuals and other authorized system components on the status of the card re-issuance process.
- (6) Verification of operation of the card, including card activation, cryptographic key generation and receipt of PKI certificates.
- (7) Interact with the applicant for verification of identity and acknowledgement of receipt of the re-issued PIV card.

3.1.3.8 Card Revocation and Termination

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

The Contractor shall have the capability to immediately process requests for revocation under the following circumstances:

- (1) The PIV card has been compromised, lost, or stolen.
- (2) The authentication credentials on the PIV card have been compromised.
- (3) An employee separates (voluntarily or involuntarily) from the Agency.
- (4) An employee separates (voluntarily or involuntarily) from the Agency's contractor.
- (5) A contractor changes positions and no longer needs access to the Agency's buildings or systems.
- (6) A PIV card holder is determined to hold a fraudulent identity or the PIV card has been fraudulent used.
- (7) A PIV card holder passes away.

The Contractor shall have the capability to ensure that revocation and termination provides the following:

- (1) Notification to the card holder, Sponsor, Issuer, other authorized agency officials, and other system services.
- (2) A process for collection of the PIV card from the card holder.
- (3) A process for destruction of the revoked and terminated PIV card.

- (4) Disposition of personal data IAW Federal laws, standards, regulations and guidelines.

The Contractor shall provide the capability to support requests 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.

3.1.3.8.1 Card Revocation and Termination Interactions

The Contractor shall have the capability to interact with other PIV systems and services as follows:

- (1) Secure receipt of request for revocation and termination and information updates from the applicant, Sponsor, and other PIV system components.
- (2) Secure receipt of authorization from the Sponsor.
- (3) Secure distribution of information to other PIV system components.
- (4) Secure receipt of information from other PIV system components.
- (5) Secure notification to authorized individuals and other authorized system components on the status of the card revocation and termination process.
- (6) Interact with the applicant for collection of the PIV card.

3.1.3.9 Card Activation and Finalization Hardware and Software Compliance

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

3.1.3.10 Card Activation and Finalization Deployment Services Compliance

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

3.1.3.11 Audit, Logging, and Standard Reporting

The Contractor shall 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 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.

3.1.3.12 Technical Standards Compliance

All data output from the card activation and finalization 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.

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 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 activation and finalization 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 card activation and finalization 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.

3.1.3.13 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.

3.1.3.14 Security Certification and Accreditation (C&A) and Re-Accreditation

The Contractor shall provide documentation of successful completion of a security audit related to card activation and finalization 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 PIV card 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.

3.1.3.14.1 Plan for Completion of Initial C&A

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

- (1) The Contractor shall complete 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 support 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:

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 2006

- (1) The Contractor shall complete C&A IAW with Office of Management and Budget Circular A-130, Appendix III; Federal Information Security Management Act (FISMA) 2002, NIST 800-79, GSA security policies, procedures, and guidelines, and the FIPS 201 that are in full force and effect as of March 1, 2006, or as subsequently revised. The documentation defining the applicable security standards and requirements for completing C&A shall be obtained from GSA.
- (2) The Contractor shall 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 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.
- (4) The Contractor shall submit a Card Activation and Finalization Security Policy as specified in FIPS 201.

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

3.1.3.14.2 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.

3.1.3.15 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.

3.1.3.16 Performance

The Contractor shall 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.

3.1.3.16.1 Hours of Operation

The Contractor shall 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.

3.1.3.16.2 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.

3.1.3.16.3 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 3.1.3.16.3-1. 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 3.1.3.16.3-1. Response Time Requirements

| Transaction/Process | Response | Constraints |
|--|------------|--|
| Identity verification, PIV card activation, key generation, and PKI certificate installation following issuance and 1:1 biometric verification – vendor provided personnel | 20 minutes | >= 95% of all transactions within response |
| Identity verification, PIV card activation, key generation, and | 15 minutes | >= 95% of all transactions within response |

| Transaction/Process | Response | Constraints |
|--|---------------------|--|
| PKI certificate installation following issuance and 1:1 biometric verification – agency provided personnel | | |
| Renewal/Re-Issuance | 20 min. | >= 95% of all transactions within response |
| Emergency Revocation Request message | 5 min. | >= 95% of all transactions within response |
| Replacement of damaged or lost PIV card | 20 min. | >= 95% of all transactions within response |
| Data transferred between authorized PIV components | 30 sec (T1 1.54 mb) | >= 95% of all transactions within response |

3.1.3.17 Customer Service Center

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

3.1.3.17.1 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.

3.1.3.17.2 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.).

3.1.3.17.3 Hours of Operation

The customer service center shall be available 24 hours a day, 7 days per week.

3.1.3.17.4 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.

3.1.3.17.5 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.

3.1.3.17.6 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.

3.1.3.17.7 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

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

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.

3.1.3.18 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.

3.1.3.19 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.

3.1.3.20 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.

3.1.3.21 Security/Privacy Requirements

3.1.3.21.1 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, card activation and finalization operators (issuers), 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.

3.1.3.21.2 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.

3.1.3.21.3 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.

3.1.3.22 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.

3.1.3.23 Deliverables

The Contractor shall have the capability to provide the following deliverables as listed in Table 3.1.3.23-1, Deliverables.

Table 3.1.3.23-1. 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 distribution 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. |
| 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. |

Card Activation and Finalization 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 | 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. |
| 9 | Record of approval to provide Homeland Security Presidential Directive 12 (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. |
| 10 | Security Audit, or Certification and Accreditation (C&A) and Re-Accreditation documentation as specified in NIST Special Publications, or a plan for C&A. | As required in qualification requirements response package. |

Card Activation and Finalization 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 |
|-----|--|---|---|---|--|
| 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 |
| 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 (1) | Electronic access, plus 1 paper copy | As required in request | Within 10 business days of the end of the month covered in the report. |

Card Activation and Finalization 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 |
|-----|--|---|---|---|---|
| 20 | Data collection forms | As required in request |
| 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. |
| 23 | Implementation plan and schedule. | As required in request. |

3.1.3.24 Project Management Office

The Contractor shall have the capability to provide a Project Management Office (PMO) to oversee all facets of the managed card activation and finalization services.

3.1.3.25 Managed Card Activation and Finalization Services Qualification Requirements Response Package Submission

The Contractor shall provide the following information and documentation in response to the card activation and finalization 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.

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006

Revised August 30, 2006

- (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 3.1.3.22 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.
- (5) Documentary evidence of competence of employees as specified in Section 3.1.3.19 of this document.
- (6) Documentary evidence of integrity and trustworthiness of employees as specified in Section 3.1.3.21.1 of this document.
- (7) Documentary evidence of security audit, C&A, or plan for C&A, as specified in Section 3.1.3.14.

See Appendix A, Qualification Requirements Submission Criteria, for additional requirements on 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.

The Contractor shall have the capability to comply with the pricing requirements specified in SIN 132-62, this qualification and requirements document, and as follows:

- (1) Pricing for card activation and finalization stations shall not include the costs for the physical space. Physical space at agency locations for card activation and finalization stations 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) Card activation and finalization hardware and software products.
- (2) Card activation and finalization deployment services.
- (3) Managed card activation and finalization 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 Activation and Finalization Services and Products Compliance Matrix as part of their response to the Statement of Qualification Requirements for PIV services and products.

Card Activation and Finalization 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"/> | Enrollment and Registration |

| | |
|--------------------------|------------------------|
| <input type="checkbox"/> | Systems Infrastructure |
| <input type="checkbox"/> | Card Production |

TECHNICAL REQUIREMENTS:

Activation and Finalization 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 |
|----------|--|---|----------------------|
| 54. | Activation and Finalization Hardware and Software Products - required for all 3 categories <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.1 | |
| 55. | Activation and Finalization Software <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Supporting Proposal Section:</div> | 3.1.1.3 | |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| | | | |
| 56. | Hardware and Software Maintenance Support – required for all 3 categories Supporting Proposal Section: | 3.1.1.5 | |
| 57. | Deliverables Supporting Proposal Section: | 3.1.1.10 | |

Activation and Finalization Deployment Services – specific requirements – Section 3.1.2

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 58. | Activation and Finalization Hardware and Software Products Compliance Supporting Proposal Section: | 3.1.2.1 | |
| 59. | Scheduling Tool– required for deployment and managed services Supporting Proposal Section: | 3.1.2.2 | |
| 60. | Training - – required for deployment and managed services Supporting Proposal Section: | 3.1.2.3 | |
| 61. | Customer Service Center – required deployment and managed services Supporting Proposal Section: | 3.1.2.4 3.1.3.12 | |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | | | |
| 62. | Availability of Services – required for deployment and managed services Supporting Proposal Section: | 3.1.2.6 | |
| 63. | Response Time for Services Supporting Proposal Section: | 3.1.2.7 | |
| 64. | Scalability and Implementation Schedule – required for deployment and managed services Supporting Proposal Section: | 3.1.2.8 | |
| 65. | Project Management Office – required for deployment and managed services Supporting Proposal Section: | 3.1.2.14 3.1.3.24 | |
| 66. | Deliverables Supporting Proposal Section: | 3.1.2.13 | |

Managed PIV Integrated Services – specific requirements - Section 3.1.3

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---------------------------|---|----------------------|
| 67. | Verification of Applicant | 3.1.3.1 | |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | Supporting Proposal Section: | | |
| 68. | Card Activation Supporting Proposal Section: | 3.1.3.2 | |
| 69. | Cryptographic Key Generation and Receipt of Certificate(s) Supporting Proposal Section: | 3.1.3.3 | |
| 70. | Post Issuance Process Supporting Proposal Section: | 3.1.3.4 | |
| 71. | Card Renewal Supporting Proposal Section: | 3.1.3.5 | |
| 72. | Card Replacement Supporting Proposal Section: | 3.1.3.6 | |
| 73. | Card Re-Issuance Supporting Proposal Section: | 3.1.3.7 | |
| 74. | Card Revocation and Termination Supporting Proposal Section: | 3.1.3.8 | |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | | | |
| 75. | Activation and Finalization Hardware and Software Compliance Supporting Proposal Section: | 3.1.3.9 | |
| 76. | Activation and Finalization Deployment Services Compliance Supporting Proposal Section: | 3.1.3.10 | |
| 77. | Scheduling Tool– required for deployment and managed services Supporting Proposal Section: | 3.1.2.2 | |
| 78. | Availability of Services – required for deployment and managed services Supporting Proposal Section: | 3.1.2.6 | |
| 79. | Scalability and Implementation Schedule – required for deployment and managed services Supporting Proposal Section: | 3.1.2.8 | |
| 80. | Training - – required for deployment and managed services Supporting Proposal Section: | 3.1.2.3 | |
| 81. | Audit, Logging, and Standard Reporting Supporting Proposal Section: | 3.1.3.11 | |

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|--|---|----------------------|
| | | | |
| 82. | Date/Time Stamp Synchronization Supporting Proposal Section: | 3.1.3.15 | |
| 83. | Performance Supporting Proposal Section: | 3.1.3.16 | |
| 84. | Customer Service Center – required for deployment and managed services Supporting Proposal Section: | 3.1.2.4 3.1.3.12 | |
| 85. | Data Transfer Supporting Proposal Section: | 3.1.3.20 | |
| 86. | Project Management Office – required for deployment and managed services Supporting Proposal Section: | 3.1.3.24 | |
| 87. | Deliverables Supporting Proposal Section: | 3.1.3.23 | |

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

Card Activation and Finalization Services and Products
Statement of Qualification Requirements

June 19, 2006
Revised August 30, 2006

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 88. | Security Certification and Accreditation (C&A) and Re-Accreditation – see Security Requirements Evaluation Form | | |
| 89. | Privacy Act Requirements – See Security Requirements Evaluation Form | | |
| 90. | Past Performance – See Past Performance Requirements Evaluation Form | | |
| 91. | Technical Standards Compliance <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Supporting Proposal Section:</div> | 3.1.1.1 3.1.3.12 | |
| 92. | Interface and Interoperability Support <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Supporting Proposal Section:</div> | 3.1.1.2 3.1.3.13 | |
| 93. | Allowance for Technology Changes <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Supporting Proposal Section:</div> | 3.1.1.7 3.1.2.9 | |
| 94. | Contractor Personnel Training <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Supporting Proposal Section:</div> | 3.1.1.8 3.1.2.11 3.1.3.19 | |
| 95. | Special Contract Requirements <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">Supporting Proposal Section:</div> | 3.1.1.6 3.1.2.5 | |

SECURITY REQUIREMENTS:

Activation and Finalization Hardware and Software Products

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 96. | Security standards requirements <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Supporting Proposal Section: </div> | 3.1.1.4 | |

Activation and Finalization Deployment Services

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 97. | Security standards requirements <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Supporting Proposal Section: </div> | 3.1.1.4 | |

Managed Activation and Finalization Services

| Req. No. | Description | Qualification Requirements Section References | Compliance Statement |
|----------|---|---|----------------------|
| 98. | Security standards requirements <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Supporting Proposal Section: </div> | 3.1.1.4 | |
| 99. | 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. | 3.1.3.14 | |

Card Activation and Finalization 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"> • Documentation of previous management Authority to Operate (ATO) on a similar system. • Plan for obtaining ATO | | |
| 100. | Privacy Act Requirements <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Supporting Proposal Section: </div> | 3.1.3.18 | |
| 101. | Administrative Personnel Security <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Supporting Proposal Section: </div> | 3.1.1.9 3.1.2.12 | |
| 102. | Security/Privacy Requirements <ul style="list-style-type: none"> • Administrative Personnel Security • Privacy Requirements • Data Retention <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Supporting Proposal Section: </div> | 3.1.3.21 | |