Attachment D
Deployment Options

The contractor must select at least one Deployment Option from the list below. When selecting a Deployment Option, please be aware of the security requirements provided. If more than one option is supported indicate the price and technical approach differences in the quote.

A. Software only - Deliver the software as an application binary and/or Amazon Machine Image (AMI) to the client and client fully manages hosting, updates, configuration, updated. Vendor provides software and maintenance updates that will be hosted and managed by the login.gov team in the login.gov environments; vendor will not have access to the login.gov environment.

B. Vendor hosted offering - Solution fully hosted by vendor in a dedicated instance that meets requirements for a moderate ATO. Vendor may propose a dedicated offering via traditional hosting or private cloud.

The vendor shall specify which deployment option(s) they support. The Contractor and the Government shall mutually agree on a deployment option (i.e., A or B) Depending on the deployment option, security requirements for Deployment Option A or B apply. If in the future, the vendor requests to transition to a Public or Community cloud hosted deployment model; the environment must first achieve FedRAMP authorization. Transitioning from either Deployment A or B to a Cloud Service Delivery model is a major change and will require close coordination with the GSA and a contractual modification to reflect the change in delivery model.

1.1. Security - Deployment Option A

Vendor shall deliver the software as an installable application package and/or Amazon Machine Image (AMI) to the Government. The vendor shall provide software updates and security patches in a timely manner with or without discovery of any vulnerabilities by the client through security scans. Major and minor releases shall be tested by the vendor and be compliant with federal release management practices. If any issues arise after applying these updates within the client's infrastructure, vendor will provide support to help resolve these issues.

The vendor will not have access into the login.gov environment; the Government fully manages software updates and access to the hosting infrastructure.

1.1.1. Enterprise User License Agreements Requirements (EULA)

The Contractor shall provide all EULA's in an editable Microsoft Office (Word) format. EULA's will be reviewed by the Government to ensure there is no conflict with any policies, rules or regulations.

1.1.2. Information Technology (IT) Acceptance

For IT solutions, including configuration and development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved through documentation updates, program correction, or other mutually agreeable methods.

1.2. Security - Deployment Option B

Vendor hosted offering - Solution fully hosted by vendor in a dedicated instance that meets requirements for a moderate ATO. Vendor may propose a dedicated offering via traditional hosting or private cloud.

1.2.1. External Contractor Information Systems - IT Security Requirements

1.2.1.1. Required Policies and Regulations for GSA Contracts

Contractors are required to comply with Federal Information Processing Standards (FIPS), the "*Special Publications 800 series*" guidelines published by NIST. Federal Information Processing Standards (FIPS) publication requirements are mandatory for use. NIST special publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems"*
- FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems"*
- FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules"*
- NIST Special Publication 800-18, *"Guide for Developing Security Plans for Federal Information Systems"*
- NIST Special Publication 800-30 Revision 1, *"Guide for Conducting Risk Assessments"*
- NIST Special Publication 800-34 Revision 1, *"Contingency Planning Guide for Federal Information Systems"*
- NIST Special Publication 800-37 Revision 1, *"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach"*
- NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*
- NIST Special Publication 800-53 Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"*
- NIST Special Publication 800-53A Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans"*

1.2.1.2. GSA Security Compliance Requirements

FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*", is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Contractor systems supporting GSA must meet the minimum security requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), "*Security and Privacy Controls for Federal Information Systems and Organizations*".

To comply with the Federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*", and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are provided in Appendix A, of this document. The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

1.2.1.3. Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The ensuing table identifies essential security controls from the respective baselines to highlight their importance and ensure they are implemented. The Contractor shall make the proposed system and security architecture of the information system available to the login.gov team, Contracting Officer, and the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	The information system routes privileged authentication traffic to external hosted infrastructures / applications through GSA's managed network access control points to subject them to the Trusted Internet Connections (TIC) and Einstein monitoring.

AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements including but not limited to: Successful and unsuccessful Account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. Web applications should log all admin activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
CM-6	Configuration Settings	L, M, H	Information systems, including vendor owned / operated systems on behalf of GSA, shall configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Amazon Web Services based architectures must implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts.
IA-2 (2)	Identification and Authentication (Organizational	M, H	FIPS PUB 199 Moderate and High impact information systems must implement multi-factor authentication for non-privileged accounts.

	Users) | Network Access to Non-Privileged Accounts		
IA-2 (12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	L, M, H	All information systems with an e-authentication assurance level of 2 or above, used by federal employees or contractors must accept federal Personal Identity Verification (PIV) cards and ensure verification.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.

RA-5	Vulnerability Scanning	L, M, H	All systems must complete monthly OS, web, and database configuration scanning and provide results to the GSA together with POA&Ms.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on EARC list.
SC-8 / SC-8 (1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. • Digital signature encryption algorithms - Reference: (http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html#Approved • Block cypher encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved • Secure hashing algorithms – Reference: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html#Approved Internet accessible Websites shall implement HTTPS Only and HTTP Strict Transport Security (HSTS), reference OMB Memorandum M-15-13. SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."* Systems shall be HTTPS only and implement HSTS.
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. • Digital signature encryption algorithms - Reference: (http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html#Approved • Block cypher encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved • Secure hashing algorithms – Reference: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html#Approved
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide

			14-69, *"SSL/TLS Implementation"*, and NIST Special Publications 800-32, NIST 800-63.
SC-18	Mobile Code	M, H	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	GSA Required – For systems with Personally Identifiable Information Only	System bearing PII must implement protect information at rest. At a minimum, fields bearing PII data must be encrypted with field level encryption. Encryption algorithms shall be FIPS-approved; implemented encryption modules shall be FIPS PUB 140-2 validated.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Moderate, High, and Critical risk findings must be remediated prior to go-live. Post go-live, All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days.
SI-3	Malicious Code Protection	L, M, H	
SI-4	Information System Monitoring	L, M, H	

SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security",* and OWASP Top 10 Web Application Security Vulnerabilities.
AR-8	Accounting of disclosures		The system keeps an accurate accounting of disclosures of PII including: date, nature, and purpose of each disclosure; and the name and address of the person or entity to which the disclosure was made.
TR-2	System of Record Notices and Privacy Act Statements		The system includes Privacy Act Statements on the forms or pages that collect PII.
UL-1	Use Limitation	M, H	The system uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
UL-2	Information Sharing with third parties	M, H	The system discloses PII externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes

1.2.1.4. Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 1 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk*", provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) at least every three (3) years or at the discretion of the Authorizing Official when there is a significant change to the system's security posture or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:

    - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems"*. The SSP shall include as appendices required policies and procedures across 18 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Agreements (in agreement with NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems")*. The SSP shall include as an appendix, a completed GSA 800-53 Control Tailoring worksheet included in Appendix A of this guide. Column E of the worksheet titled "Contractor Implemented Settings" shall document all contractor implemented settings that are different from the GSA defined setting and where the GSA defined setting allows a contractor determined setting.
    - Contingency Plan (including Disaster Recovery Plan) completed in agreement with NIST Special Publication 800-34.
    - Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
    - Plan of Actions & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."*
    - Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all FIPS PUB 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS PUB 199 High impact information systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37 Revision 1, "Guide for the Security Certification and Accreditation of Federal Information Systems", and CIO IT Security 06-30, "Managing Enterprise Risk " or via continuous monitoring based on GSA CIO IT Security 12-66, "Information Security Continuous Monitoring Strategy" that is reviewed and accepted by the GSA CISO.

3. At the Moderate impact level and higher, the contractor will be responsible for providing an independent Security Assessment/Risk Assessment and Penetration Test in accordance with GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk."

4. The Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct its own security assessment and penetration testing (as necessary) to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk". Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.

5. Identified gaps between required 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)." Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.

6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (Security Authorization Package (SAP)) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), system Program Manager (PM), Information System Security Manager (ISSM), and Information System Security Officer (ISSO) will render an authorization decision to:
   - Authorize system operation w/out any restrictions or limitations on its operation;
   - Authorize system operation w/ restriction or limitation on its operation, or;
   - Not authorize for operation.

2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review.

If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

1.2.1.5. Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided to the GSA COR/ISSO/ISSM Monthly

1. Vulnerability Scanning

   Reference: NIST 800-53 control RA-5
   Provide monthly vulnerability scan reports from Web Application, Database, and Operating System Scans. Scan results shall be managed and mitigated in Plans of Action and Milestones (POA&Ms).

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

1. Plan of Action & Milestones (POA&M) Update

   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M)*".

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

1. Updated A&A documentation including the System Security Plan and Contingency Plan

2. System Security Plan

   Reference: NIST 800-53 control PL-2
   Review and update the System Security Plan annually to ensure the plan is current and accurately described implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

3. Contingency Plan

Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, "Contingency Planning Guide."

4. User Certification/Authorization Review Documents

   Reference: NIST 800-53 control AC-2
   Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

5. Separation of Duties Matrix

   Reference: NIST 800-53 control AC-5
   Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

6. Information Security Awareness and Training Records

   Reference: NIST 800-53 control AT-4
   Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

7. Annual FISMA Assessment

   Reference: NIST 800-53 control CA-2
   Deliver the results of the annual FISMA assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation*". The assessment is completed using the GSA on-line assessment tool.

8. System(s) Baseline Configuration Standard Document

   Reference: NIST 800-53 control CM-2
   Provide a well-defined, documented, and up-to-date specification to which the information system is built.

9. System Configuration Settings

   Reference: NIST 800-53 control CM-6

Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements.
Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.

10. Configuration Management Plan

    Reference: NIST 800-53 control CM-9
    Provide an annual update to the Configuration Management Plan for the information system.

11. Contingency Plan Test Report

    Reference: NIST 800-53 control CP-4
    Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the "Low Impact" level. The table top test must include Federal and hosting Contractor representatives. Moderate and High impact systems must complete a functional exercise at least once every three years.

12. Incident Response Test Report

    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

13. Results of Physical Security User Certification/Authorization Review

    Reference: NIST 800-53 control PE-2
    Provide the results of annual reviews and validations of physical access authorizations to facilities supporting the contractor system to ensure the continued need for physical access.

14. Results of Review of Physical Access Records

    Reference: NIST 800-53 control PE-8
    Provide the results of annual reviews and validations of visitor access records to ensure the accuracy and fidelity of collected data.

15. Information System Interconnection Agreements

    Reference: NIST 800-53 control CA-3

Provide updated Interconnection Security Agreements (ISA) and supporting Memorandum of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems"*, for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. Interconnections agreements shall be submitted as appendices to the System Security Plan.

16. Rules of Behavior

    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

17. Personnel Screening and Security

    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order 2100.1 – *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1 – "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.
    - Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
    - Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
    - Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

    Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

    Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

1. Policies and Procedures

Develop and maintain current the following policies and procedures:

a. Access Control Policy and Procedures (NIST 800-53 AC-1)
b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
l. Key Management Policy (NIST 800-53 SC-12)

1.2.1.6. Additional Stipulations (as applicable)

1. The deliverables shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*

2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.

4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services

for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.