

Attachment 1: Excerpts from GSA Security Requirements

Access to Documents: The GSA policy documents referenced herein and the excerpts provided contain the information necessary for Offerors to propose under the GSA SmartPay 3 Master Contract. These policies are not available for distribution or publication. Offerors may make an appointment to view hardcopy documents in person at GSA, 1800 F Street, Washington DC, through the GSA Contracting Officer, Donna Rankin, by sending an email to donna.rankin@gsa.gov. Appointments must be requested in writing within 7 calendar days of the issuance of the solicitation and must be completed no later than 21 days prior to the date / time set for receipt of proposals. Appointment dates will be assigned and confirmed on a first come, first served basis. Offerors will be provided instructions for access to the GSA building at time of confirmation of their appointment. The number of attendees from the Offeror is limited to not more than four (4) persons employed by the Offeror or their proposed subcontractors / team members, due to limited conference room space. Offerors will be monitored by a Government employee at all times while in custody of the documents. Offerors may take notes but may not take photos or photocopy any documents.

1 External Contractor Information Systems – It Security Requirements

1.1 Required Policies and Regulations for GSA Contracts

Contractors entering into an agreement for services to the General Services Administration (GSA) and/or its Federal customers shall be contractually subject to all GSA and Federal IT Security standards, policies, and reporting requirements. The contractor shall meet and comply with all GSA IT Security Policies and all applicable GSA and NIST standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

All GSA contractors must comply with the current version of the GSA policies below (these documents are all referenced within the GSA IT Security Policy) (access to all documents immediately below will be provided by GSA upon request):

- GSA Information Technology (IT) Security Policy (CIO 2100.1)
- Homeland Security Presidential Directive-12 (HSPD- 12) Personal Identity Verification and Credentialing (GSA Order CIO 2181.1)
- GSA Information Technology (IT) General Rules of Behavior (GSA Order CIO 2104.1A)
- GSA Privacy Act Program (GSA Order CPO 1878.1)
- GSA IT Security Procedural Guide: Contingency Planning (CIO IT Security 06-29)
- GSA IT Security Procedural Guide: Managing Enterprise Risk (CIO IT Security 06-30)
- GSA IT Security Procedural Guide: Plan of Action and Milestones (CIO IT Security 09-44)
- GSA IT Security Procedural Guide: Continuous Monitoring Program (CIO IT Security 12-66)
- GSA IT Security Procedural Guide: SSL/TLS Implementation (CIO IT Security 14-69)
- GSA IT Security Procedural Guide: Web Application Security Guide (CIO IT Security 07-35)
- GSA IT Security Procedural Guide: Conducting Penetration Test Exercises (CIO IT Security 11-51)
- GSA IT Security Procedural Guide: FISMA Implementation (CIO IT Security 04-26)
- GSA IT Security Procedural Guide: Incident Handling (CIO IT Security 01-02)

Contractors are also required to comply with Federal Information Processing Standards (FIPS), the “Special Publications 800 series” guidelines published by NIST, and the requirements of FISMA outlined below (all documents immediately below are publicly available through Internet search):

- Federal Information Security Modernization Act of 2014
- Clinger-Cohen Act of 1996 also known as the “Information Technology Management Reform Act of 1996.”

- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors”
- Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources”, and Appendix III, “Security of Federal Automated Information Systems”, as amended.
- OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies.”
- 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 Information Technology 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.”

All documents referenced in the above Section may be replaced by more recent versions, as specified by the GSA Office of the Chief Information Security Officer.

1.2 GSA Security Compliance Requirements

FIPS 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), and “Recommended Security Controls for Federal Information Systems.

To comply with the Federal standard, GSA must determine the security category of the information and information system in accordance with FIPS 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 199 impact level are provided, as are other internal Guides and Regulations available for review by controlled access.

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. Guidelines to establish a system banner on login to the EAS shall be met on a best effort basis and solution submitted

for approval by GSA. In reference to OMB requirements for Agencies to implement Trusted Internet Connections (TIC) the contractor systems are considered an External System and access to Agency networks will be managed following Government Agencies established access and/or connections requirements under TIC or other applicable regulations that supports secure connections to Agency networks and systems.

1.3 Essential Security Controls

All NIST 800-53 R4 controls must be implemented as per the applicable FIPS 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 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) and if currently built be reviewed before any government data is processed or held on the system.

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	
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. Web applications should log all admin activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.
CA-8	Penetration testing	GSA Required	Information systems must undergo an independent third party penetration test as part of the security assessment.
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 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).

Control ID	Control Title	Baseline	GSA Implementation Guidance
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 Users) Network Access to Non-Privileged Accounts	M, H	FIPS 199 Moderate and High impact information systems must implement multi-factor authentication for non-privileged accounts.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS 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 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 140-2 certified encryption module during transport outside of controlled areas.
RA-5	Vulnerability Scanning	L, M, H	All information system must complete quarterly OS, web, and database configuration scanning and provide results to the GSA together with POA&Ms.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-8 / SC-8(1)	Transmission Confidentiality and Integration	M, H	<p>Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS 140-2 validated, respectively.</p> <ul style="list-style-type: none"> o Digital signature encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html#Approved o Block cypher encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved o Secure hashing algorithms – Reference: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html#Approved <p>SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, SSL/TLS Implementation. Systems shall be HTTPS only and implement HSTS.</p>
SC-13	Cryptographic Protection FIPS Validated Cryptography	L, M, H	<p>Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS 140-2 validated, respectively.</p> <ul style="list-style-type: none"> o Digital signature encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html#Approved o Block cypher encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved o Secure hashing algorithms – Reference: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html#Approved
SC-17	PKI Certificates	M, H	<p>Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, SSL/TLS Implementation, OMB Memorandum 05-24, and NIST Special Publications 800-32, NIST 800-63.</p>
SC-18	Mobile Code	M, H	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	<p>Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant as per 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.</p>
SC-28 (1)	Protection of Information at Rest Cryptographic Protection	GSA Required – For systems with Personally Identifiable Information Only	<p>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 140-2 validated.</p>

Control ID	Control Title	Baseline	GSA Implementation Guidance
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Moderate, High, and Critical risk findings (CVSS base Score ≥ 7.0) must be remediated prior to Authorization to Operate (ATO). Post go-live, All critical and high vulnerabilities (CVSS base Score ≥ 7.0) 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 Web Application Security Guide: (CIO-IT Security-07-35) Rev. 3 - 04/08/20016, and OWASP Top 10 Web Application Security Vulnerabilities
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.

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. All NIST 800-53 controls must be tested/assessed every 3 years or as defined by GSA policy.

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 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 Plan Testing."
 - 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 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS 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 ."
 3. At the Moderate impact level and higher, the contractor or Government (as determined in the contract) will be responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk."
 4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities 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 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.

1.5 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 COTR/ISSO/ISSM Quarterly

1. Plan of Action & Milestones (POA&M) Update
Reference: NIST 800-53 control CA-5
Contractor shall 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."
2. Vulnerability Scanning
Reference: NIST 800-53 control RA-5
Contractor shall provide 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) and submitted together with the quarterly POA&M submission.

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

1. Updated A&A documentation including the System Security Plan and Contingency Plan
 - a. *System Security Plan*
Reference: NIST 800-53 control PL-2
Contractor shall 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.
 - b. *Contingency Plan*
Reference: NIST 800-53 control CP-2
Contractor shall provide an annual update to the contingency plan completed in accordance with NIST 800-34, Contingency Planning Guide.
2. User Certification/Authorization Review Documents

Reference: NIST 800-53 control AC-2

Contractor shall 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.

3. Separation of Duties Matrix

Reference: NIST 800-53 control AC-5

Contractor shall 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.

4. Information Security Awareness and Training Records

Reference: NIST 800-53 control AT-4

Contractor shall 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.

5. Annual FISMA Assessment

Reference: NIST 800-53 control CA-2

Contractor shall deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation". The assessment is completed using the GSA provided assessment tools on each FY.

6. System(s) Baseline Configuration Standard Document

Reference: NIST 800-53 control CM-2

Contractor shall provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings

Reference: NIST 800-53 control CM-6

Contractor shall 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.

8. Configuration Management Plan

Reference: NIST 800-53 control CM-9

Contractor shall provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report

Reference: NIST 800-53 control CP-4

Contractor shall provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, "Contingency Plan Testing." 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.

10. Incident Response Test Report

Reference: NIST 800-53 control IR-3

Contractor shall provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, "Incident Handling."

11. Results of Physical Security User Certification/Authorization Review

Reference: NIST 800-53 control PE-2

Contractor shall 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.

12. Results of Review of Physical Access Records

Reference: NIST 800-53 control PE-8

Contractor shall provide the results of annual reviews and validations of visitor access records to ensure the accuracy and fidelity of collected data.

13. Information System Interconnection Agreements

Reference: NIST 800-53 control CA-3

The contractor shall 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.

14. Rules of Behavior

Reference: NIST 800-53 control PL-4

Contractor shall define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

15. Personnel Screening and Security

Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA order 2100.1 – IT Security Policy and GSA Order CIO P 2181 – HSPD-12 Personal Identity Verification (PIV) and Credentialing Handbook. The PIV requirements may not apply to all contractor personnel and the three categories of personnel discussed below shall be submitted and approved by GSA as to what risk level an employee work access may fall under. 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).

The Contracting Officer, through the Contracting Officer’s Technical Representative or Program Manager will ensure that a completed Contractor Information Worksheet (CIW) for each Applicant is forwarded to the Federal Protective Service (FPS) in accordance with the GSA/FPS Contractor Suitability and Adjudication Program Implementation Plan dated 20 February 2007. FPS will then contact each Applicant with instructions for completing required forms and releases for the particular type of personnel investigation requested.

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 COTR/ISSO/ISSM Biennially

1. Policies and Procedures - Contractor shall 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 CIO IT Security Procedural Guide 01-02, Incident Handling)
 - 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)

1.6 Additional Stipulations (as applicable)

1. The deliverables identified in Sections 1.4 and 1.5 shall be labeled “CONTROLLED UNCLASSIFIED INFORMATION” (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of For Official Use Only (FOUO) and CUI to or from a GSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, “Security requirements for Cryptographic Modules.”
2. *United States Government Configuration Baseline (USGCB)*: 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, updates, 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. As prescribed in the Federal Acquisition Regulation (FAR) clause 24.104, if the system involves the design, development, or operation of a system of records on individuals, the contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act."
4. 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.
5. 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. In accordance with the FAR clause 52.239-1, 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 Task Ordering Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this Task Order or otherwise provided by the Government. Exception example- Disclosure to a Consumer Agency for purposes of A&A verification.
 - b. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government logical and physical access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
 - 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.

- c. 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. At a minimum, the Government ISSO must be notified when contractor discover the threats or hazards to include unauthorized release of PII or CUI information.

1.7 Exceptions

Exceptions to GSA Security Requirements contained herein and the referenced documents are as follows:

1. Implementation of PIV card authentication;
2. Implementation of TIC; and

3. Implementation of the GSA warning banner. GSA will accept the contractor's generic warning banners.

2 Internal Contractor or Government Information Systems - IT Security Requirements

2.1 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 Revision 1, "*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*"

2.2 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. Where a GSA security hardening benchmark exists, it must be used. GSA security hardening benchmarks may be exceeded but not lowered. GSA benchmarks are available on the GSA Intranet and will be provided by the GSA upon request.

2.3 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; ensure they are implemented; and identify integration requirements with GSA's IT and IT Security environment (if any). Contractor systems shall ensure these essential security controls are implemented. Further, the Contractor shall make the proposed system and security architecture of the information system available to 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	Account management systems must leverage or integrate seamlessly with an existing GSA Access and Identity Management Solution such as GAMS, PIV-based authentication, or other GSA-supported Single-Sign-On solution.
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 as documented in applicable GSA IT Security Technical Hardening Guides 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. Internal Information systems shall in near-real time transmit audit log events to GSAs Security Incident and Event Management (McAfee ESM v. 9.6.0).
CM-6	Configuration Settings	L, M, H	GSA information systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate, may be used. Further, all workstations and servers connected to the GSA network integrate with BigFix and have agents installed.
CP-7	Alternative Processing	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across

Control ID	Control Title	Baseline	GSA Implementation Guidance
	Site		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. Internal systems including those hosted in GSA supported cloud environments shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).
IA-2 (2)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts	M, H	Information systems at the FIPS PUB 199 Moderate and High impact levels must implement multi-factor authentication for non-privileged accounts. Internal systems including those hosted in GSA supported cloud environments shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).
IA-2 (12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	L, M, H	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-

Control ID	Control Title	Baseline	GSA Implementation Guidance
			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 integrate with the GSA vulnerability scanning tool set (currently Nessus) managed by the Security Operations Division in the Office of the Chief Information Security Officer. Information systems shall coordinate integration with the scanning program by contacting SecOps@gsa.gov. The scan team will require a detailed system inventory identifying all assets/devices in scope of the information system boundary and authentication information for access.
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 Integration	M, H	<p>Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively.</p> <ul style="list-style-type: none"> o Digital signature encryption algorithms - Reference: (http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html#Approved) o Block cypher encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved o Secure hashing algorithms – Reference: http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html#Approved <p>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.”</p>

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-13	Cryptographic Protection	L, M, H	<p>Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively.</p> <ul style="list-style-type: none"> o Digital signature encryption algorithms - Reference: (http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html#Approved) o Block cypher encryption algorithms - Reference: http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html#Approved o 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, “ <i>SSL/TLS Implementation</i> ”, and NIST Special Publications 800-32, NIST 800-63.
SC-18	Mobile Code	M, H	iOS and Android app creation, usage restrictions. Mobile applications shall undergo assessment and authorization practices as documented in GSA IT Security Procedural Guide 12-67, “ <i>Securing Mobile Devices and Applications.</i> ”
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	L, M, H	All internal or internal-cloud systems must

Control ID	Control Title	Baseline	GSA Implementation Guidance
	Code Protection		incorporate Bit9 and FireEye HX agents on supported systems. These agents will be provided; external systems must implement malicious code protection software for all in scope operating systems.
SI-4	Information System Monitoring	L, M, H	All information systems must be monitored internally and across ingress/egress points for potentially malicious activity. In addition, all internal or internal-cloud systems must incorporate Bit9 and FireEye HX agents on supported Windows operating systems. These agents will be provided by GSA during the design and implementation of the solution. These agents will need to be able to establish network connectivity to the GSA-owned controllers.
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.

2.4 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 IT Security Procedural Guide 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 GSA 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 or Government (as determined in the contract) will be responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk*."
 4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities 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 Assessment 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.

2.5 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

- a. 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.*"

- b. 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.*"

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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. GSA information systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate, may be used.

All workstations and servers connected to the GSA network integrate with BigFix and have agents installed.

8. Configuration Management Plan

Reference: NIST 800-53 control CM-9

Provide an annual update to the Configuration Management Plan for the information system.

9. 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.

10. 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*."

11. 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.

12. 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.

13. 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.

14. 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.

15. 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 – "*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)

2.6 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.

3 Cloud Information Systems – IT Security Requirements

The preparation of the deliverables in this contract will be completed at a Controlled Unclassified Information (CUI) level. The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*" (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

3.1 Assessment and Authorization

GSA may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (JAB Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

3.2 Assessment of the System

1. The contractor shall comply with FedRAMP 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 documentation using FedRAMP requirements and templates, which are available at <https://www.fedramp.gov/>:

- Privacy Impact Assessment (PIA)
 - FedRAMP Test Procedures and Results
 - Security Assessment Report (SAR)
 - System Security Plan (SSP)
 - IT System Contingency Plan (CP)
 - IT System Contingency Plan (CP) Test Results
 - Plan of Action and Milestones (POA&M)
 - Continuous Monitoring Plan (CMP)
 - FedRAMP Control Tailoring Workbook
 - Control Implementation Summary Table
 - Results of Penetration Testing
 - Software Code Review
 - Interconnection Agreements/Service Level Agreements/Memorandum of Agreements
2. Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
 3. The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
 4. 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. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.
 5. Physical Access Considerations – If the Cloud Service Provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
 6. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a GSA authorization is issued.
 7. The contractor is responsible for mitigating all security risks found during 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.

3.3 Authorization of the System

1. If the CSP SaaS or PaaS is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP website - <http://www.fedramp.gov/marketplace/compliant-systems/>); GSA will leverage the CSPs FedRAMP Assessment and Authorization package to document and assess the customer controls for which GSA has responsibility and issue a GSA ATO for the agency's instance of the CSPs SaaS offering. The CSP shall work with the GSA to facilitate documentation and assessment of required customer controls, as necessary.
2. If the Cloud Service Provider (CSP) Software as a Service (SaaS) or Platform as a Service (PaaS) offering is NOT already FedRAMP authorized, it shall:
 - a. Operate on an Infrastructure as a Service (IaaS) CSP environment that is FedRAMP authorized; AND
 - b. Be listed as FedRAMP In Process on the FedRAMP Website - <http://www.fedramp.gov/marketplace/in-process-systems/>, OR be listed as FedRAMP Ready on the FedRAMP website - <http://www.fedramp.gov/marketplace/fedramp-ready-systems/>
3. CSP shall ensure these essential security controls are implemented. CSP shall implement FedRAMP parameters control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to 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 (as applicable)) and/or the start as A&A activities.

Control ID	Control Title	FedRAMP Baseline
AC-2	Account Management	L, M, H
AU-2	Audit Events	L, M, H
CM-6	Configuration Settings	L, M, H
CP-7	Alternative Processing Site	M, H
CP-8	Telecom Services	M, H
IA-2 (1)	Identification and Authentication (Organizational Users) Network Access to Privileged Accounts	L, M, H
IA-2 (2)	Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts	M, H
IA-2 (12)	Identification and Authentication (Organizational Users) Acceptance of PIV Credentials	L, M, H
IA-7	Cryptographic Module Authentication	L, M, H
MP-4	Media Storage	M, H
MP-5	Media Transport	M, H
PL-8	Information Security Architecture	M, H

Control ID	Control Title	FedRAMP Baseline
RA-5	Vulnerability Scanning	L, M, H
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity Cryptographic or Alternate Physical Protection	M, H
SC-13	Cryptographic Protection	L, M, H
SC-17	PKI Certificates	M, H
SC-18	Mobile Code	M, H
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H
SC-28 (1)	Protection of Information at Rest Cryptographic Protection	M, H
SI-2	Flaw Remediation	L, M, H
SI-3	Malicious Code Protection	L, M, H
SI-4	Information System Monitoring	L, M, H
SI-10	Information Input Validation	M, H

4. If the CSP SaaS is NOT FedRAMP authorized at the time of contracts award BUT is operated on an IaaS environment that is FedRAMP authorized and is identified as either FedRAMP In Process or FedRAMP Ready on the FedRAMP website; THEN the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, GSA may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another Federal Department/Agency or be based on the GSA Moderate SaaS process as described in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." The CSP shall make available any existing assessment and authorization package for GSA review and provide necessary documentation and access to facilitate the GSA SaaS A&A process.

3.4 Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes 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 in agreement with FedRAMP guidelines and submitted to the MAX.Gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

The contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization (if necessary) to achieve FedRAMP authorization. Deliverables shall include:

- Monthly OS, web, and database vulnerability scans (deliverable shall include raw results and findings shall be included in the POA&M document);
- Quarterly Plan of Action and Milestones (POA&M);
- Annual A&A Package updates including the System Security Plan, Contingency Plan, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, GSA will accept the FedRAMP A&A and continuous monitoring documentation made available on the MAX.Gov Portal or a repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

3.5 Personnel Security Requirements

Contractor shall 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 – “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.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

3.6 Sensitive Information Storage

Controlled Unclassified Information (CUI) information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, “Guidelines for Media Sanitization.” The destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

3.7 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as Controlled Unclassified Information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

3.8 Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

3.9 Personally Identifiable Information

The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

Privacy data (should it come into scope) will require that the vendor's cloud solution be FedRAMP authorized at the FIPS PUB 199 moderate level.

3.10 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

3.11 Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

3.12 Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

3.13 Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

3.14 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

3.15 Additional Stipulations

1. The FedRAMP 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 contractor shall comply with any additional FedRAMP privacy requirements.
5. 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. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

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.

3.16 References

- Guide to Understanding FedRAMP: <https://www.fedramp.gov/files/2015/03/Guide-to-Understanding-FedRAMP-v2.0-4.docx>
- FedRAMP Cloud Computing Documents: <https://www.fedramp.gov/resources/documents-2016/>
- FedRAMP Templates: <https://www.fedramp.gov/resources/templates-2016/>

4 Mobile Application - IT Security Requirements

The preparation of the deliverables in this contract will be completed at a Controlled Unclassified Information (CUI) level. The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy" (or current version) and GSA IT Security Procedural Guide 12-67, "Securing Mobile Devices and Applications", or current version. In situations where there are no procedural guides, the

contractor shall use generally accepted industry best practices for IT security.

4.1 General Mobile Application Guidelines

1. The App shall be integrated with an MDM (Mobile Device Management) solution. GSA currently uses MAAS 360.
2. The contractor shall provide to the GSA IT Contracting Officer Representative (COR) the source code and all supporting artifacts of the app for security testing via the GSA Static and mobile Code Scanning program. GSA currently uses the HP Fortify tool for static code reviews and Checkmarx for mobile code. In addition, the contractor shall actively participate in the program to remediate all findings according to the most recent Static Code Scanning Standard Operating Procedure SOP before the beta and production App is accepted by GSA. Once the contract is awarded, GSA will provide a copy of the Static Code Scanning SOP to the contractor.
3. The contractor shall provide clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App. All source code information prepared for this App is the property of GSA, Federal Acquisition Service, OCCM and GSA IT.
 - The contractor shall provide detailed process and code documentation.
 - The contractor shall provide Mobile App features documentation.
 - The contractor shall support development and updates of a security authorization package for the App following the process requirements documented in GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications*", or current version.

4.2 Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications*", which will be provided upon contract award.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. But as mobile app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you don't have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required
- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple iTunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated and approved by the AO for the system they support before deployment

4.3 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple iTunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an OS of a mobile device grants a user or application root level access to the Operating System (OS). While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM.

As such, the following policies apply to all GSA devices (Government and Bring Your Own Device) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation
- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android.

The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below:

- Apple iTunes App Review guidelines - <https://developer.apple.com/appstore/guidelines.html>
- Google Play Store App Review guidelines - <http://developer.android.com/distribute/googleplay/publish/index.html>

4.4 Terms of Service (ToS) and Privacy Discipline

Many terms found in commercial TOS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

Apps deemed to be acceptable are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the app is not mandated by the agency. Therefore, acceptance of the ToS falls upon the user as an individual. This is true even if the app is loaded using a GSA.gov domain account or registered with a user's GSA.gov email address.

Apps that are approved after formal assessment: and include a formal review by GSA Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for GSA.

Privacy considerations must be addressed, both in the use of publicly available applications, but just as importantly, those applications developed by GSA for use by GSA personnel and the general public.

As such, the following guidelines are to be adhered to:

Commercial applications – When reviewed for acceptability, consideration should be given when/if Personally Identifiable Information (PII) is collected. This review should ensure an adequate privacy notification is given to users prior to their use of the app on what data is being collected and for what purposes, as well as how it might be used by those collecting it. If the app uses GSA data, a Privacy Impact Assessment (PIA) should be generated for that app and filed for consideration by the Privacy

Office for GSA. If it is determined that a System of Records Notice (SORN) is required, a full assessment of the app itself and underlying systems should be conducted prior to use.

GSA developed applications – A GSA developed mobile app should undergo all the same reviews procedures and practices given to any developed application on any other platform. This should be documented in the PIA and System Security Plan for which the mobile app is a part of and a Privacy Notice must be included on the home screen of the mobile app itself.

If the app does NOT collect PII, at a minimum, the Privacy Notice should indicate that to the user. This can be done by taking the user to another screen on the app prior to launch or by any means that allows a user to close the app prior to use before they are taken to an interactive screen.

If the mobile app DOES collect PII, the following minimum guidelines should be adhered to and addressed in the Privacy Notice as outlined above.

Privacy Statement

*This mobile application does collect your personal information. We collect (*developer insert information here*). Your personal information is collected so we can (*developer insert information here*). Your personal information is stored in (*developer insert information here*) GSA system. If you need more information, go to GSA Privacy Act SORN site.*

4.5 GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

1. A GSA developed app that supports a GSA FISMA system must be documented in the System Security Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. GSA IT Security Procedural Guide 06-30, “*Managing Enterprise Risk*”, is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have an assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).
2. Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS’ for GSA developed mobile apps for all releases.
3. All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 of GSA IT Security Procedural Guide 12-67, “*Securing Mobile Devices and Applications*” and the release process documented in this section.
4. Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
5. The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.
6. Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division (ISE) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is

authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.

7. All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for developing OWASP is outlined below:
 - a. OWASP Security Testing Guide Link - https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
 - b. OWASP Mobile Security Project Home Page - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
 - c. OWASP Secure Development considerations https://www.owasp.org/images/0/04/Security_Testing_Guidelines_for_mobile_Apps_-_Florian_Stahl%2BJohannes_Stroeher.pdf
8. GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.
9. Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security Plan for the system they support.
10. Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the GSA Office of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. Apps must have a Privacy Threshold Analysis (PTA), and if applicable a PIA (templates are available at the links below) tied to either an existing SORN or have a new one initiated and approved by the GSA Privacy Office and Office of General Counsel.

[Privacy Threshold Analysis Template](#)

[Privacy Impact Assessment Template](#)

3. A mobile application security assessment review (template available in Section 8.7 of the document linked below) must be completed and signed by the mobile app owner, mobile app assessor, mobile app Information System Security Manager (ISSM), a representative of the Office of the CSIO, to denote a proper assessment and review was conducted of the mobile app prior to release.

[GSA IT Security Procedural Guide 12-67, "Securing Mobile Devices and Applications"](#)

4.6 Intellectual Property

This task order is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of this task order, and a "paid-up" nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this task order.

4.7 Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

4.8 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

4.9 Personnel Security Requirements

Contractor shall 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 – “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.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

4.10 Additional Stipulations

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.