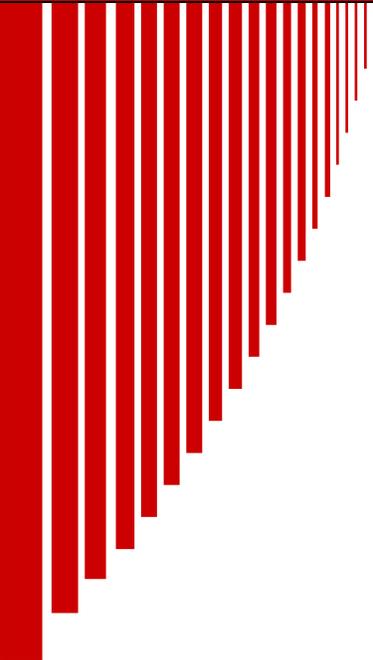


**Security Language for IT Acquisition  
Efforts  
CIO-IT Security-09-48**



## VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change

### Approval

CIO IT Security Procedural Guide CIO-IT Security-09-48, Security Language for IT Acquisition Efforts, is hereby approved for distribution.



Signed: \_\_\_\_\_

Date: 09/10/2009

# Table of Contents

<b>INTRODUCTION .....</b>	<b>4</b>
<b>SCOPE.....</b>	<b>5</b>
<b>PURPOSE .....</b>	<b>5</b>
<b>CONTRACT LANGUAGE .....</b>	<b>6</b>
1.1. Required Policies and Regulations for GSA Contracts.....	6
1.2. GSA Security Compliance Requirements.....	7
1.3. Certification and Accreditation (C&A) Activities .....	8
1.4. Reporting and Continuous Monitoring .....	10
1.5. Additional Stipulations (as applicable).....	15
<b>APPENDIX A: GSA TAILORING OF NIST 800-53 CONTROLS.....</b>	<b>17</b>

## Introduction

The U.S. General Services Administration (GSA) must provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act (FISMA) describes Federal agency security responsibilities as including “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.” This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency, Information systems used or operated by an agency or other organization on behalf of an agency. Office of Management and Budget (OMB) Memorandum M-09-29, “FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management”, identifies five primary categories of contractors as they relate to securing systems and information: 1) service providers, 2) contractor support, 3) Government Owned, Contractor Operated facilities (GOCO), 4) laboratories and research centers, and 5) management and operating contracts.

The security contract language identified in this guide should be inserted in all Statements of Work where the information system is contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).. GSA Program Managers and acquisition management organizations with the procurement process are responsible for ensuring that the solicitation document includes the appropriate information security requirements. The information security requirements must be sufficiently detailed to enable service providers to fully understand the information security regulations, mandates, and requirements that they will be subject to under the contract or task order that may be awarded to them. This will also give potential contractors a better opportunity to ask questions about these Information Technology (IT) security requirements. The idea is to better prepare contractors and Commercial Service Providers to be compliant with GSA and Federal IT security requirements up front, avoiding unnecessary future contract modifications. Contractors systems, upon entering into a contractual agreement for services to GSA, will be subject to GSA policies, procedures, testing, reporting requirements, and general scrutiny.

The following sections are intended to be used “as is” and are appropriately formatted to allow this language to be placed in-line within a statement of work.

NOTE: FIPS 199 High impact and Cloud computing contracts involving subscription services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Storage as a Service (SaaS), or Software as a Service (SaaS) shall be coordinated through the Office of the Senior Agency Information Security Officer (OSAISO). Such services have added complexity that may require additional controls not found in this guide that may be required to protect to the degree required by FISMA, FISMA implementing standards, and associated guidance.

## Scope

The security requirements identified in this guide are specific to contractor owned and operated systems on behalf of GSA or the Federal Government (when GSA is the managing agency). OMB Memorandum M-09-29 asserts that agencies are responsible for ensuring information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the National Institute of Standards and Technology (NIST).

## Purpose

The purpose of this document is to define and establish consistent language for GSA IT acquisition contracts involving contractor owned and operated systems to ensure compliance with the appropriate provisions of FISMA, OMB Circular A-130, and NIST 800-53 R3. Each of the sections below highlights a key element of GSA's IT security objectives for contractor acquisition efforts.

# Contract Language

## 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 GSA policies below (these documents are all referenced within the GSA IT Security Policy).

- GSA Information Technology (IT) Security Policy, CIO P 2100.1E.
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook”, dated October 20, 2008.
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior”, dated July 3, 2003.
- GSA Order CPO 1878.1, “GSA Privacy Act Program”, dated October 27, 2003.
- GSA IT Security Procedural Guide 04-26, “FISMA Implementation”.
- GSA IT Security Procedural Guide 06-29, “Contingency Plan Testing”.
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”
- GSA IT Security Procedural Guide 08-39, “FY 2009 IT Security Program Management Implementation Plan.”
- GSA IT Security Procedural Guide 09-44, “Plan of Action and Milestones (POA&M).”

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.

- Federal Information Security Management Act (FISMA) of 2002.
- 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”, August 27, 2004.
- 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 Rev 1, “Guide for Developing Security Plans for Federal Information Systems.”
- NIST Special Publication 800-30, “Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems.”
- NIST Special Publication 800-34, “Contingency Planning Guide for Information Technology Systems.”
- NIST SP 800-37, Revision 1, “Guide for the Security Certification and Accreditation of Federal Information Systems.”
- NIST Special Publication 800-47, “Security Guide for Interconnecting Information Technology Systems.”
- NIST Special Publication 800-53 Revision 3, “Recommended Security Controls for Federal Information Systems.”
- NIST Special Publication 800-53A, “Guide for Assessing the Security Controls in Federal Information Systems.”

## 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 3 (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 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, as deemed appropriate by the Authorizing Official.

### **1.3. Certification and Accreditation (C&A) Activities**

The implementation of a new Federal Government IT system requires a formal approval process known as Certification and Accreditation (C&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", give guidelines for performing the C&A process. The Contractor system/application must have a valid certification and accreditation (signed off by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid certification and accreditation will be grounds for termination of the contract. The system must have a new C&A conducted (and signed off on 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 no less than every 3 years.

#### ***Certification of System***

1. The Contractor shall comply with Certification and Accreditation (C&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 C&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 C&A documentation:
  - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1. 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). 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)."

- Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities.

In addition to the above documentation, GSA recommends (not a requirement) the contractor employ code analysis tools to examine the software for common flaws and document results in a Code Review Report. The Code Review Report should be submitted as part of the C&A package. Reference NIST 800-53 control SA-11, Enhancement 1 for additional details.

2. Information systems must be certified and accredited at least 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 certification and accreditation (C&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 C&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.

### ***Accreditation of System***

1. Upon receipt of the documentation (Certification Package) 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 Senior Agency Information Security Officer (SAISO), system Program Manager, Information System Security Manager (ISSM), and Information System Security Officer (ISSO)) will render an accreditation 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.

#### **1.4. 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 authorizing officials 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 C&A documentation including the System Security Plan and Contingency Plan
  - i. 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.
  - ii. 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 on-line assessment tool.

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. System configuration settings will be updated or reviewed on an annual basis.
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 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).

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:
  - i. Access Control Policy and Procedures (NIST 800-53 AC-1)
  - ii. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
  - iii. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
  - iv. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
  - v. 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)
  - vi. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
  - vii. Media Protection Policy and Procedures (NIST 800-53 MP-1)
  - viii. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
  - ix. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
  - x. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
  - xi. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
  - xii. Key Management Policy (NIST 800-53 SC-12)

## 1.5. Additional Stipulations (as applicable)

1. The deliverables identified in section 1.4 shall be labeled “CONTROLLED UNCLASSIFIED INFORMATION” (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of 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. Federal Desktop Core Configuration  
The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 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 FDCC 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 FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC 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 Federal Acquisitions Regulations (FAR) clause 52.239-1, the Contractor shall be responsible for the following privacy and security safeguards:
  - i. 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 - Disclosure to a Consumer Agency for purposes of C&A verification. <List any other exceptions as necessary>*

- ii. 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:
  - o Authenticated and unauthenticated operating system/network vulnerability scans
  - o Authenticated and unauthenticated web application vulnerability scans
  - o 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.

- iii. 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.

## Appendix A: GSA Tailoring of NIST 800-53 Controls

Click on the attached workbook to open.



GSA 800-53 Control  
Tailoring\_FINAL.xls