

Attachment (X)

Offeror's Certification of Understanding of Security Publications / Affirmation of Offeror's Information Security Policies

The government requires that information technology solutions meet Federal security standards. Security standards and specifications will be provided at the Task level and 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, and 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.”

In addition to being able to perform in accordance to the referenced publications as required at the Task level, an Offeror must affirm that the Offeror's information security policies, procedures, and practices applicable to all information systems it owns or operates which contain, transmit, or process information provided by or generated for the Government to support the operations and assets of a Federal agency (“Federal Information”), which may be reasonably contemplated to be used during the performance of this contract, meet, at a minimum, the requirements of the security control baseline for Low-Impact information systems (in the most current version of NIST Special Publication 800-53), or conform to the requirements commercial standards that provide a substantially equivalent or greater level of security.

If the Offeror is making this certification based on conformance to standards other than those in the most current version of NIST Special Publication 800-53, Offeror shall list those standards and describe how conformance to them meets or exceeds the security control baseline for Low-Impact information systems. The list and description shall be appended to and incorporated by reference into this certification and affirmation, and Offeror shall indicate such incorporation below.

Nothing in this certification and affirmation creates a requirement for the Offeror to submit a System Security Plan for these systems, or for the government to provide Certification and Accreditation or Authorization to Operate the Offeror's systems which contain, transmit, or process Federal Information.

External transmission/dissemination of FOUO and CUI to or from Offeror's systems which contain, transmit, or process Federal Information must be encrypted. Certified

encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."

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, updates, 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.

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."

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.

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:

- 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.

- 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.
- iv. In the event of a breach of Federal Information, the contractor shall report the breach and any relevant details to the Government within 72 hours.

Certification of Understanding of Security Publications / Affirmation of Offeror's Information Security Policies

I hereby certify the Offeror's understanding of security publications and do affirm that the Offeror's information security policies, procedures, and practices applicable to all information systems it owns or operates which contain, transmit, or process information provided by or generated for the Government to support the operations and assets of a Federal agency ("Federal Information"), which may be reasonably contemplated to be used during the performance of this contract, meet, at a minimum, the requirements of the security control baseline for Low-Impact information systems (in the most current version of NIST Special Publication 800-53), or conform to the requirements of a commercial standard that provides a substantially equivalent or greater level of security.

_____ Signature

_____ Date

_____ Printed Name

_____ Title

Appendix of conformance to commercial standards included? Yes _____ No
