DRAFT

Publication 4812
State of Security (SoS) Package

Contractor Security Controls

Handling and Protecting

Information or Information Systems

******This Package Pertains to IT Assets Owned and Managed at Contractor Sites******

January 2014

The Need for Contractor Security Controls

Inside this SoS Package

The E-Government Act of 2002 (Public Law 107-347) Title III, Federal Information Security Management Act (FISMA) of 2002 requires each agency to provide 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." FISMA requires federal agencies to develop and implement policies for information security oversight of contractors and other users with access to federal information and information systems.

Because of requirements distinct to Internal Revenue Service (IRS) mission objectives, as well as specific laws or rulings, such as the Gramm-Leach Bliley (GLB) Act, the Federal Trade Commission (FTC) Financial Privacy Rule and Safeguards Rule, and the Sarbanes-Oxley Act, IRS contractors, their affiliates, subcontractors, and service providers are subject to additional requirements for protecting information and information systems, when appropriate or applicable.

Publication 4812 defines basic security controls, requirements and standards that apply to contractors, contractor employees, subcontractors, and subcontractor employees supporting the primary contract, based on the security controls framework under National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Revision 3), Recommended Security Controls for Federal Information Systems and Organizations, as amended, where those contractor employees have access to, develop, operate, or maintain IRS information or information systems. While NIST SP 800-53 (Revision 3), as amended, is a general guide, the intent of Publication 4812 is to provide IRS security requirements in the IRS contracting environment.

For all contracts subject to this publication that are 12 months or more in duration (inclusive of the base period and/or any exercised option periods), and the value of which is greater than the Simplified Acquisition Threshold (currently $150,000 as defined in FAR Part 2) (inclusive of the value of the base period and all options), the contractor shall develop and submit a State of Security (SoS) package each period of performance of the contract (base and exercised option periods), or once every 12 months, whichever period

The SoS package shall be furnished to the Contracting Officer's Representative (COR) (or the Contracting Officer (CO) if no COR is appointed) no later than 60 calendar days after the effective date of the contract in the base period (typically, the award date, unless specified otherwise), and on or before the annual anniversary of the effective date of the contract in each exercised option period. Note: If the base period is less than 60 calendar days in duration, the initial submission is still due within 60 days of the effective date of the contract (although it technically falls in the first option period), and the next submission is still due on or before the annual anniversary of the effective date of the contract (although it too technically falls in the first option period). Any information submitted electronically for the SoS package shall be encrypted and sent to Pub4812@irs.gov

Instructions

Administrative Data: Provides the data required to identify the contractor, the IRS Contracting Officer, the IRS Contracting Officer's Representative, as well as the contract for which the SoS is being completed. The data in this section is self explanatory with the following notes:

1. Place of Performance if Different from Location of Facility: Identify the specific location where the work on the contract is being performed if it is different than the contractor address/location of facility.
2. Contract Purpose: Provide a brief statement that describes what the contract entails. For example: The purpose of the contract is to provide support in processing taxpayer revenues. This includes all income and expenses.

Subcontractor and/or Service Provider Information: Provide the name and address of any subcontractor that will support the IRS contract.

Security Environment Indicators: This section is used to provide a high level determination of the type of information being processed in support of the contract, the security control level that contract falls under, if the data is available on a public facing website, and if there has been a contract review in the past 3 three years for this or another IRS contract/order.

1. Returns or Returns Information: Identify if the contract includes the processing or any taxpayer returns or return information. If yes, determine the volume. Volume is determined by the number of individual returns or return information processed during a specified period of time. For example, 1,000,000 taxpayer returns annually. The contract will usually provide the answer to this question.
2. Personally Identifiable Information (PII): If the answer was yes to tax payer returns, then this number will generally be the same. In the case of return information, the number could be different. For example, the tax return data only contains metrics, but not any personally identifiable information such as name, address, taxpayer identification number. The type of return information and number will determine the volume of PII being processed. The contract will usually provide the answer to this question.
3. Law Enforcement Sensitive (LES) Data: LES data is defined as any data collected, processed, and/or stored in the support of law enforcement activities. For example, data collected regarding fraudulent tax returns. The contract will usually

4. Security Control Level: The term Security Control Level is used in Appendix C of Publication 4812 to describe categories/levels such as Core (C), Core Simplified Acquisition Threshold (CSAT), Core Networked Information Technology (CNET) and Core Software Application Development (CSOFT). For additional information, please refer to Publication 4812 Appendix C.

Publically Facing Website: Publically facing websites are defined as websites that are available to the general public over the Internet. If such a website is used to support the contract, answer yes and identify the URL (website name/address).

Previous Contract Review: Identify if there has been an IRS contract review in the last 3 years for this or another IRS contract/order. If yes, then complete the remaining questions. When and where it was completed and the contract number it was completed for. Determine if there were any vulnerabilities/security weaknesses identified and if any POA&Ms exist. In general POA&Ms identify the weakness and the strategy/plan to mitigate identified vulnerabilities/weaknesses.

IT Environment: Provides information on how IRS data is processed in support of the contract. Respond yes or not to each question.

1. Self explanatory.
2. Determine if the IT system being used to support the IRS contract is wholly owned and managed by internal sources. If yes, than the answer is no. If a third-party source is used, for example: the servers are located in a third-party datacenter, then the answer is yes. The answer would also be yes if you use any third-party vendor to provide maintenance or other support for servers that support the IRS contractor.
3. Answer yes if IRS data is either physically or logically separated from any other data being processed on the IR system.
4. Determine if a plan is in place and documented to destroy or sanitize all IRS sensitive information /data from computers, devices, and electronic and information technology upon contract termination.
5. Self Explanatory.

Backup/Contingency

1. Answer yes if backups that contain IRS data are physically or logically segregated from backups containing any other data.
2. Is your backup media encrypted using FIPS 140-2 standards?
3. Answer yes, if the alternate processing or storage facility is located outside of the United States. Please identify any offshore location that is not a U.S. territory.
4. Please enter the address and location of your backup media/devices.

Additional Comments: Use this section to respond to any open ended questions where additional space is needed.

SoS Questionnaire

The SoS Questionnaire consists of a series of closed ended questions. Note: Preference for POC is the Contractor Security Representative.

A. ADMINISTRATIVE INFORMATION
1. Contractor Name:
2. Contractor Address/Location of Facility:
3. Place of Performance if Different From Location of Facility:
4. Point of Contact (POC) Name:
5. POC Telephone Number:
6. POC Email Address:
7. Business Website/URL:
8. IRS CO and COR:
9. Contract/Order Number:
10. Contract/Order Short Title:
11. Contract Purpose (Please provide two sentences describing the purpose):
12. Period of Performance (base/base plus all options):
13. Dollar Value (base/base plus all options):
14. Business Size (# of staff supporting the contract):
15. Date Questionnaire Completed:

Note: Preference for POC is the Contractor Security Representative.

B. SUBCONTRACTOR and/or SERVICE PROVIDER INFORMATION
1. Subcontractor 1 Name:
2. Address:
1. Subcontractor 2 Name:
2. Address:
3. Subcontractor 3 Name:

C. SECURITY ENVIRONMENT INDICATORS	YES	NO	N/A
Does the site/place of performance handle or process any of the following types of information?			
1. Returns or return information? If yes, indicate volume?			
a) The number of taxpayer records housed at the facility?			
2. PII? If yes, indicate volume?			
a) Law Enforcement Sensitive Information? If Yes, please provide explanation.			
3. What security control level does your contract fall within (i.e., C, CSAT, CNET, and CSOFT)?			
4. Are you currently operating or maintaining a public facing website for IRS/ Treasury?			
a) If yes, web site name, e.g. HTTP address?			
5. Has IRS Contractor Security Assessments (CSA) conducted a security assessment under the contract order (or another IRS contract/order) within the last 3 years of the date questionnaire completed?			
a) If yes, when/where/contract number?			
6. If Yes, is there a Plan of Action & Milestones (POA&M)?			
a) Date of Last POA&M Update? Provide a POA&M.			

C. SECURITY ENVIRONMENT INDICATORS	YES	NO	N/A
7. Has an independent third-party Security assessment been conducted? If yes provide information e.g. who, what, where and when.			
8. Is there a plan/procedure in place to ensure all information is returned to the IRS and to ensure all information is sanitized and/or destroyed when being retained on IT computer assets?			

Note: As needed, add rows for subcontractors with access to IRS information.

D. IT ENVIRONMENT	YES	NO	N/A
1. Are you using workstations/desktop computers to store or process IRS sensitive information?			
2. Are you using file servers to store or process IRS sensitive information?			
3. Is Microsoft Active Directory, or similar tool, being used to manage server/ workstation environments?			
4. Does you partition or segregate IRS information/data from that of other customers/clients?			
5. Do you have automated tools to enable hard drives to be degaussed and/or wiped, when data is no longer required, hardware is broken, or when the contract ends?			

E. BACKUP/CONTINGENCY	YES	NO	N/A
1. Are all backups that contain SBU data segregated from all other backups?			
2. Is all backup media encrypted?			
3. Are backups maintained in a facility other than the production facility?			
4. Is there alternate processing or storage facility used for SBU data located outside of the United States?			
a) Alternate Backup Address:			

SoS Questionnaire (continued)

F. ADDITIONAL COMMENTS

Contractor Security Reviews are conducted by IRS and cannot be a self-assessment performed by the contractor. Contractor Statements of Security Assurance (CSSA) to be completed by contractors, as described hereinafter; however, do provide the means for the contractor to make a preliminary assertion to the IRS as to its' perceived level of conformity to security requirements. Such assessments/assertions can provide contractors further insight into their own operating environments, and serve as one of the tools used to determine if and when a Contractor Security Review will be performed by the IRS on any given contract, in any given annual review cycle.

The IRS shall employ CSSAs as part of an integrated security management approach to proactively mitigate security risks. IRS shall use a staged report card or traffic light information system in its assessment of contractor reporting to augment compliance reviews (i.e., Contractor Security Reviews). CSSAs are not required for contracts subject to Publication 4812 that are less than 180 days in duration. CSSAs are required for all contracts subject to Publication 4812 that are between 180 days and 12 months in duration and in which there are no options to extend the term of the contract. Contractors in this group are required to submit a CSSA to the COR during the period of performance according to the following schedule:

- For contracting actions with a start date on or after July 1st, not later than December 31st of that same year, or 180 days after the award date; whichever date is later.
- For contracting actions with a start date after January 2nd, not later than June 30th of that same year, or 180 days after the award date, whichever date is later.

The CSSA, available at the following site http://www.irs.gov/uac/Publication-4812----Contractor-Security-Controls, is in the format of an electronic questionnaire that includes a dropdown menu that allows the user to select the version of the CSSA associated with the security control level applicable to the immediate contract.

Assurance

The Contractor Statement of Physical Security Assurance (CSPSA) is the IRS security management approach to the Physical Security in proactively mitigating security risks. The CSPSA is a companion form to the CSSA and is required as part of the SoS Package. (see requirement guidance for the CSSA)

The CSPSA, available at the following site http://www.irs.gov/uac/Publication-4812-–-Contractor-Security-Controls, is in the format of an electronic questionnaire that includes a dropdown menu that allows the user to select the version of the CSPSA associated with the security control level applicable to the immediate contract.

System Security Plan

The contractor shall develop and maintain a security plan to identify key information about the contractor site and about the security controls that shall be used to ensure that IRS information is adequately safeguarded.

Security plans are designed to document the security controls surrounding an information system environment. The contractor security plan shall ensure that security controls surrounding the contractor site environment have been adequately documented and safeguard mechanisms are in place.

Each year, the contractor shall provide a State of Security Package, that includes a contractor System Security Plan (SSP) to the IRS. The SSP will include the following:

- **Administrative Information Cover:** Include information such as contractor name, location of facilities handling IRS SBU information or information systems, points of contract (e.g., Project Manager, Information System Administrator, Security Officer) (to include telephone number and email address), contract/order number, period(s) of performance, dollar value (by performance periods), business size and socioeconomic characteristics, etc.
- **Employee Roster:** Identify all contractor employees working on the contract, and annotate those that have access to or handle SBU information, or have access to or operate or work with information systems containing SBU information. In addition, verify which contractor employees have or have not completed the current annual requirements for the Security Awareness Training.
- **Subcontractor Support:** Names and addresses of contractor and all subcontractors performing IRS work.
- **Infrastructure Diagram:** Provide a diagram providing a general picture of the IT assets being used.
- **Inventory of IT Assets:** Provide an inventory of the type of equipment being used, including IT equipment/component, number of components, associated serial numbers, and location.

Additional reference information for completing a security plan can be obtained from the NIST Web site: NIST SP 800-18 Revision 1, Developing Security Plans for Federal Information Systems.