

SUPPORTING STATEMENT FOR PAPERWORK REDUCTION ACT SUBMISSION 3090-0300, IMPLEMENTATION OF INFORMATION TECHNOLOGY SECURITY PROVISION

A. Justification

1. Administrative requirements.

The General Services Administration (GSA) is extending an existing OMB information collection, requiring contracting officers to insert the clause at 552.239-71, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts containing the provision at 552.239-70, Information Technology Security Plan and Accreditation. As such, the provision and clause are inserted in solicitations that include information technology supplies, services or systems in which the contractor will have physical or electronic access to government information that directly supports the mission of GSA. The clause requires contractors, within 30 days after contract award, to submit an IT Security Plan to the Contracting Officer and Contracting Officer's Representative for acceptance that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under the contract.

The plan must describe those parts of the contract to which this clause applies. The Contractors IT Security Plan shall comply with applicable Federal laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures. GSA's Office of the Chief Information Officer issued "CIO IT Security Procedural Guide 09-48, Security Language for Information Technology Acquisitions Efforts," to provide IT security standards, policies and reporting requirements. This document is incorporated by reference in all solicitations and contracts or task orders where an information system is contractor owned and operated on behalf of the Federal government. The guide can be accessed at <http://www.gsa.gov/portal/category/25690>. Specific security requirements not specified in "CIO IT Security Procedural Guide 09-48, Security Language for Information Technology Acquisitions Efforts" shall be provided by the requiring activity. The plan shall be consistent with and further detail the approach contained in the contractor's proposal or sealed bid. The plan shall be incorporated into the contract as a compliance document.

The contractor shall comply with the accepted plan.

Six months after contract award, the contractor shall submit written proof of IT security accreditation for acceptance by the Contracting Officer. The accreditation must be in accordance with NIST Special Publication 800-37.

On an annual basis, the contractor shall submit verification to the Contracting Officer that the IT Security plan remains valid.

This provision was added to the General Services Administration Acquisition Regulations (GSAR) to implement a recommendation from the Office of the Inspector General (OIG) based on an internal audit of the security of GSA's information technology data and systems. The audit recommended that GSA develop standard requirements and deliverables for IT service contracts and task orders that promote compliance with GSA IT Security Policy and Procedures.

2. Use of information. GSA will use this information to verify that the contractor shall secure GSA's information technology data and systems from unauthorized use.

3. Use of information technology. We use improved information technology to the maximum extent practicable. Where both the Government and the contractor are capable of electronic interchange, these information collection requirements may be submitted electronically.

4. Describe efforts to identify duplication. The reporting requirements placed on contractors are not duplicative of any other language in the Federal Acquisition Regulation (FAR) or the General Services Administration Acquisition Regulation (GSAR).

5. If the collection of information impacts small businesses describe any methods used to minimize the burden.

The collections associated with small businesses are the minimum consistent with applicable laws, Executive orders, and prudent businesses practices. The information required to prepare the IT Security Plan, submit written proof of IT security accreditation six months after award, and verify that the IT Security Plan remains valid annually, will be collected, as needed, from both large and small businesses. The nature of the reporting requirements precludes reducing the information collection burden for small businesses. Comments are requested from large and small business concerns and other interested parties on this issue.

6. Describe the consequences to Federal activities if the collection is not conducted or is conducted less frequently. Failure to require the submission of the IT Security Plan may result in noncompliance with IT security requirements in accordance with Federal and GSA policies and procedures. Such noncompliance creates the potential for GSA's information assets being exposed to undue risks of inappropriate disclosure, destruction, and alteration.

The requirement to have the contractor submit written proof of IT security accreditation to the Contracting Officer within six months of contract award further guarantee's the security of GSA's information technology data and systems.

Collecting information on the annual verification of a valid IT Security Plan will also help to ensure the security of GSA's information technology data and systems.

7. Special circumstances for collection. Collection of information on a basis other than by individual contractors is not practical. The contractor is the only one who has the records necessary for the collection. We will not collect information in a manner that requires an explanation of special circumstances. Collection is consistent with the guidelines in 5 CFR 1320.6.

8. Efforts to consult with persons outside the agency. A 60 day notice was published in the *Federal Register* at 79 FR 54722 on September 12, 2014. No comments were received. A 30 day notice was published in the *Federal Register* at 79 FR 70533 on November 26, 2014. No comments were received.

9. Explanation of any decision to provide any payment or gift to respondents, other than remuneration of contractors or guarantees. We will not provide any payment or gift to respondents to this information collection requirement.

10. Describe assurance of confidentiality provided to respondents. We will disclose the information collected only to the extent consistent with prudent business practices, current regulations, and in accordance with the requirements of the Freedom of Information Act. We do not provide an assurance of confidentiality to respondents.

11. Additional justification for questions of a sensitive nature. No sensitive questions are involved.

12. **Estimated total annual public hour burden.** We used information generated from the Federal Procurement Data System (FPDS) (using fiscal year (FY) 2012 and 2013 data) to determine the number of contractors performing information technology services for GSA under contracts and task orders. We retrieved contracts and task orders valued at \$25,000 or more awarded using the PSC code D - ADP and Telecommunication Services from FPDS. Based on the FY12 FPDS data collected there were 102 unique DUNS numbers for such contract actions, and based on the FY13 FPDS data collected there were 104 unique DUNS numbers. The average unique DUNS numbers for FY12 and FY13 on such contract actions is 103.

We estimated 5 hours for responding to this request due to several factors. First, we conducted research of other agencies' regulations to determine if they had similar information technology security requirements. We found three agencies have the same requirement; Department of State, Department of Transportation, and NASA) and that this requirement was implemented as far back as five years ago. Based on this data, we concluded that industry should be familiar with the requirements of the GSA clause because other agencies have similar requirements. In addition, GSA's Office of the Chief Information Officer issued "CIO IT Security Procedural Guide 09-48, Security Language for Information Technology Acquisitions Efforts in November 2009. Although there is no contract clause, GSA contractors were required to meet GSA's IT security policy and guidance as stated in the guide. Finally, Federal laws and guidance such as FISMA, Office of Management and Budget Circulars, and NIST publications elude to these requirements. Therefore, this should not be a large burden because industry is familiar with the requirements.

The 5 hours per response includes the time to collect information, develop the IT security plan, report on the security accreditation six months award, and validate the IT Security plan annually.

We estimated 2 responses per respondent. We believe this is the average number of contract actions respondents will have to report on per year.

Based on aforementioned information, we estimate the total burden as follows--

Number of respondents	103
Responses per respondent	2

Number of responses	206
Avg. hours per response	<u>x 5</u>
Estimated hours	1,030

13. **Estimated total annual public cost burden.** Provide an estimate of the total annual cost burden to respondents or record-keepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12.)

Respondents:	103*
<u>Responses per respondent:</u>	<u>x 2</u>
Total annual responses:	206
<u>Preparation hours per response:</u>	<u>x 5**</u>
Total burden hours:	1,030
<u>Average hourly wages(\$50.00+36% overhead):</u>	<u>x\$68.00</u>

Total annual recordkeeping cost	\$70,040
---------------------------------	----------

* The average unique DUNS numbers for FY12 and FY13 on such contract actions is 103. We estimated 2 responses per respondent. We believe this is the average number of contract actions respondents will have to report on per year.

**Estimated time to research, analyze, and retain data to: 1) maintain an IT Security Plan; 2) report under the continuous monitoring plan; 3) comply with the accepted accreditation documentation; 4) submit annual verification that the IT Security plan remains valid; 5) ensure contractor personnel possess the appropriate security requirements to access Government systems; 6) ensure contractor personnel obtained IT security training; 7) afford the Government access to the Contractor's and subcontractors' documentation; and 8) notify the Contracting Officer when an employee either begins or terminates employment when that employee has access to GSA information systems or data. This estimate assumes automation of contractor records.

14. Estimated cost to the Government. We used information generated from FPDS (using FY12 and FY13 data), and estimates of processing times from contracting professionals. We estimate the total cost as follows--

Number of responses	206
Avg. hours per response	<u>x 2</u>
Estimated Hours	412
Cost per hour	<u>x \$41.07</u>
Total annual Government cost	\$16,920.84

The cost of \$41.07 per hour is based on the GS-12, step 5 salary. (Salary Table 2014-DCB Washington-Baltimore-Northern Virginia, DC-MD-VA-WV-PA Effective January 2014).

15. Explain reasons for program changes or adjustment reported in Item 13 or 14. Using data generated from the Federal Procurement Data System (FPDS) for FY12 and FY13, GSA was able to reduce burden hours as the number of respondents has decreased.

16. Outline plans for published results of information collection. We will not publish the results of this information collection.

17. Approval not to display expiration date. We do not seek approval not to display the expiration date for OMB approval of the information collection.

18. Explanation of exception to certification statement. Not applicable.

B. Collections of Information Employing Statistical Methods.

We will not tabulate results or employ statistical methods.