



---

August 2014

# INFORMATION SECURITY

## Agencies Need to Improve Oversight of Contractor Controls

# GAO Highlights

Highlights of [GAO-14-612](#), a report to congressional requesters

## Why GAO Did This Study

Federal agencies often rely on contractors to operate computer systems and process information on their behalf. Federal law and policy require that agencies ensure that contractors adequately protect these systems and information.

GAO was asked to evaluate how well agencies oversee contractor-operated systems. The objectives of this report were to assess the extent to which (1) selected agencies oversee the security and privacy controls for systems that are operated by contractors on their behalf and (2) executive branch agencies with government-wide guidance and oversight responsibilities have taken steps to assist agencies in ensuring implementation of information security and privacy controls by such contractors. To do this, GAO selected six agencies based on their reported number of contractor-operated systems and two systems at each agency using a non-generalizable random sample for review, analyzed agency policies and procedures, and examined security and privacy-related artifacts for selected systems. GAO also interviewed agency officials, and reviewed federal guidance and evaluated agency FISMA submissions.

## What GAO Recommends

GAO is recommending that five of the six selected agencies develop procedures for the oversight of contractors and that OMB clarify reporting instructions to agencies. The five agencies generally agreed with the recommendations and OMB did not provide any comments.

View [GAO-14-612](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov).

August 2014

## INFORMATION SECURITY

### Agencies Need to Improve Oversight of Contractor Controls

## What GAO Found

Although the six federal agencies that GAO reviewed (the Departments of Energy (DOE), Homeland Security (DHS), State, and Transportation (DOT), the Environmental Protection Agency (EPA) and the Office of Personnel Management (OPM)) generally established security and privacy requirements and planned for assessments to determine the effectiveness of contractor implementation of controls, five of the six agencies were inconsistent in overseeing the execution and review of those assessments, resulting in security lapses. For example, in one agency, testing did not discover that background checks of contractor employees were not conducted. The following table shows the degree of implementation of oversight activities at selected agencies.

**GAO Evaluation of Agency Oversight of Selected Contractor-Operated Systems**

	Establish requirements	Plan assessment	Execute assessment	Review assessment
DOE	●	◐	◐	◐
DHS	●	●	●	●
State	◐	◐	◐	◐
DOT	◐	●	◐	◐
EPA	●	●	●	◐
OPM	●	●	◐	●

Source: GAO analysis of agency data. | GAO 14 612

● Fully Implemented      ◐ Partially Implemented      ○ Not Implemented

A contributing reason for these shortfalls is that agencies had not documented procedures for officials to follow in order to effectively oversee contractor performance. Until these agencies develop, document, and implement specific procedures for overseeing contractors, they will have reduced assurance that the contractors are adequately securing and protecting agency information.

The Office of Management and Budget (OMB), the National Institute of Standards and Technology, and the General Services Administration have developed guidance to assist agencies in ensuring the implementation of security and privacy controls by their contractors. However, OMB guidance to agencies for categorizing and reporting on contractor-operated systems is not clear on when an agency should identify a system as contractor-operated and therefore agencies are interpreting the guidance differently. In fiscal year 2012, inspectors general from 9 of the 24 major agencies found data reliability issues with agencies' categorization of contractor-operated systems. Without accurate information on the number of contractor-operated systems, OMB assistance to agencies to help improve their cybersecurity posture will be limited and OMB's report to Congress on the implementation of the Federal Information Security Management Act (FISMA) is not complete.

---

# Contents

---

Letter		1
	Background	4
	Agency Oversight of Contractor-Operated Systems Was Not Always Consistent	13
	Government-wide Guidance for Contractor-Operated Systems Needs Improvement	20
	Conclusions	25
	Recommendations for Executive Action	26
	Agency Comments and Our Evaluation	27
Appendix I	Objectives, Scope, and Methodology	29
Appendix II	Comments from the Department of Energy	31
Appendix III	Comments from the Department of State	33
Appendix IV	Comments from the Environmental Protection Agency	35
Appendix V	Comments from the Office of Personnel Management	36
Appendix VI	Comments from the Department of Homeland Security	37
Appendix VII	GAO Contact and Staff Acknowledgments	38

---

---

Tables

Table 1: IT Contractual Relationships Identified by OMB for Federal Information Security Management Act Reporting	5
Table 2: Examples of Risks to Federal Systems and Data from Contractors	7
Table 3: System Oversight Activities and Key Steps from NIST Special Publications 800-35 and 800-37	12
Table 4: GAO Evaluation of Agency Oversight of Selected Contractor-Operated Systems	14
Table 5: OMB Memoranda on Contractor Oversight	21

---

Figure

Figure 1: Total IT Security Personnel Reported by Agencies for Fiscal Year 2012	6
---	---

---

**Abbreviations**

CIO	Chief Information Officer
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAR	Federal Acquisition Regulation
FISMA	Federal Information Security Management Act of 2002
GSA	General Services Administration
IT	information technology
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management
OMB	Office of Management and Budget
PIA	privacy impact assessment
POA&M	plan of action and milestones

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



August 8, 2014

The Honorable Thomas R. Carper  
Chairman  
The Honorable Tom Coburn, M.D.  
Ranking Member  
Committee on Homeland Security and Governmental Affairs  
United States Senate

The Honorable Bennie G. Thompson  
Ranking Member  
Committee on Homeland Security  
House of Representatives

The Honorable Susan M. Collins  
United States Senate

The federal government relies on information technology (IT) systems to provide essential services affecting the health, economy, and defense of the nation. The security of computer networks and systems, including federal information systems, continues to be an issue of pressing concern for the nation. We have identified the protection of federal information systems as a government-wide high-risk area since 1997 and, in 2003, expanded this high-risk area to include the protection of systems supporting the nation's critical infrastructures.<sup>1</sup> Since that time, we have issued numerous reports making recommendations to address weaknesses in federal information security programs.

Agencies frequently use the services of contractors to operate and secure computer systems and process information on their behalf. For fiscal year

---

<sup>1</sup>See GAO, *High Risk Series: An Overview*, [GAO/HR-97-1](#) (Washington, D.C.: February 1997) and *High Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: January 2003).

---

2012, the Chief Financial Officers Act agencies<sup>2</sup> reported that 33 percent of all personnel performing IT security duties were contractors.<sup>3</sup> In our prior work,<sup>4</sup> we found that agencies identified additional risks in using contractor-operated systems that may impact the privacy and security of their information and systems.

The Federal Information Security Management Act of 2002 (FISMA),<sup>5</sup> Privacy Act of 1974,<sup>6</sup> and implementing policies and guidance from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST),<sup>7</sup> require agencies to ensure the adequate protection of agency information, including information collected or maintained by contractors, as well as information systems operated by contractors on the agencies' behalf.<sup>8</sup>

You asked us to evaluate how well agencies oversee contractor-operated systems. The objectives of this report were to assess the extent to which

---

<sup>2</sup>The 24 major departments and agencies covered by the *Chief Financial Officers Act* are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

<sup>3</sup>OMB, *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*, (Washington, D.C.: March 2013).

<sup>4</sup>GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, [GAO-05-362](#) (Washington, D.C.: Apr. 22, 2005).

<sup>5</sup>As relevant here, 44 U.S.C. § 3544(a)(1)(A), (b).

<sup>6</sup>5 U.S.C. § 552a(m)(1).

<sup>7</sup>NIST provides technical leadership for the nation's measurement and standards infrastructure, including the development of management, administrative, technical, and physical standards for the security of information in federal information systems. NIST's 800-series of special publications focuses on research, guidelines, and outreach efforts in information system security.

<sup>8</sup>Other laws, such as the *E-Government Act of 2002*, the *Internal Revenue Code*, and the *Health Insurance Portability and Accountability Act of 1996*, as well as implementing policies, help to ensure the protection and privacy of certain personally identifiable, taxpayer, or personal health information that contractors may access by requiring an agency analysis of protections and risks, or by specifying the conditions or circumstances under which the information may be used or disclosed.

---

(1) selected agencies oversee the security and privacy controls for systems that are operated by contractors on their behalf, and (2) executive branch agencies with government-wide guidance and oversight responsibilities have taken steps to assist agencies in ensuring implementation of information security and privacy controls by such contractors.

For our first objective, we selected six agencies (the Environmental Protection Agency (EPA), the Departments of Energy (DOE), Homeland Security (DHS), State, and Transportation (DOT), and the Office of Personnel Management (OPM)) based on their reported number of contractor operated systems and evaluated their security and privacy policies and procedures for agency information, systems, and contractors. At each agency, we selected two systems using a non-generalizable random sample from a list of agency provided contractor-operated systems that were identified as having personally identifiable information and as either government-owned and contractor-operated and contractor-owned and contractor-operated. We evaluated how effectively the agency's assessments of security and privacy policies and procedures were being implemented at each selected system. We interviewed officials from each of the agencies' Office of the Chief Information Officer (CIO), procurement offices and program-level offices. We reviewed the agencies' respective inspector general evaluations regarding contractor oversight and included their results where appropriate.

For our second objective, we reviewed OMB guidance and instructions, DHS guidance and reports, reports from the Offices of Inspector General of the 24 Chief Financial Officers Act agencies, NIST security publications, and General Services Administration (GSA) guidance. We conducted interviews with agency officials at OMB, DHS, NIST, and GSA to identify how they assisted agencies with overseeing contractor implementation of security and privacy controls. We also interviewed officials from offices of inspectors' general of the agencies we reviewed for the first objective to discuss how the agencies are reporting their inventory of systems.

We conducted this performance audit from February 2013 to July 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and

---

conclusions based on our audit objectives. For more details on our objectives, scope, and methodology, see appendix I.

---

## Background

The use of IT is pervasive in the federal government as agencies have become dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report information. As our past work has shown, protecting federal systems and the information on them is essential because the loss or unauthorized disclosure or alteration of the information can lead to serious consequences and can result in substantial harm to individuals and the federal government. Specifically, ineffective protection of IT systems and information can result in

- threats to national security, economic well-being, and public health and safety;
- loss or theft of resources, including money and intellectual property;
- inappropriate access to and disclosure, modification, or destruction of sensitive information;
- use of computer resources for unauthorized purposes or to launch an attack on other computer systems;
- damage to networks and equipment;
- loss of public confidence; and
- high costs for remediation.

While some incidents can be resolved quickly and at minimal cost, others may go unresolved and result in significant costs.

---

## Agencies Rely on Contractors to Operate and Secure Systems

Federal agencies rely extensively on contractors to provide IT services and operate systems to help carry out their missions. For example, we reported that in fiscal year 2012, the Department of Defense obligated approximately \$360 billion for contracts for goods and services, such as information technology and weapon systems maintenance.<sup>9</sup> The ability to contract for technology services can allow an agency to obtain or offer enhanced services without the cost of owning the required technology or maintaining the human capital required to deploy and operate it. Specifically, contractors and their employees provide services and systems to agencies at agency and contractor facilities, directly and by

---

<sup>9</sup>GAO, *High Risk Series: An Update*, [GAO-13-283](#) (Washington, D.C.: February 2013).



---

remote access. Services can include computer and telecommunication systems and services, and testing, quality control, installation, and operation of computer equipment.

OMB guidance<sup>10</sup> defines five primary categories of contractor relationships associated with securing systems and information: (1) service providers; (2) contractor support; (3) government-owned, contractor-operated facilities; (4) laboratories and research centers; and (5) management and operating contracts. Table 1 describes the five types of contractual relations identified by OMB.

---

**Table 1: IT Contractual Relationships Identified by OMB for Federal Information Security Management Act Reporting**

<b>Contractor category</b>	<b>Description of services</b>
Service providers	Typical outsourcing of system or network operations, telecommunication services, or other managed services (including those provided by another agency and subscribing to software services).
Contractor support	On or off-site contractor technical or other support staff.
Government-owned, contractor-operated facilities	Agency component whose security requirements are identical to those of the managing federal agency.
Laboratories and research centers	Agency component whose security requirements are identical to those of the managing federal agency.
Management and operating contracts	Contracts for the operation, maintenance, or support of a government-owned or controlled research, development, special production, or testing establishment.

Source: OMB Memoranda 14-4. | GAO-14-612

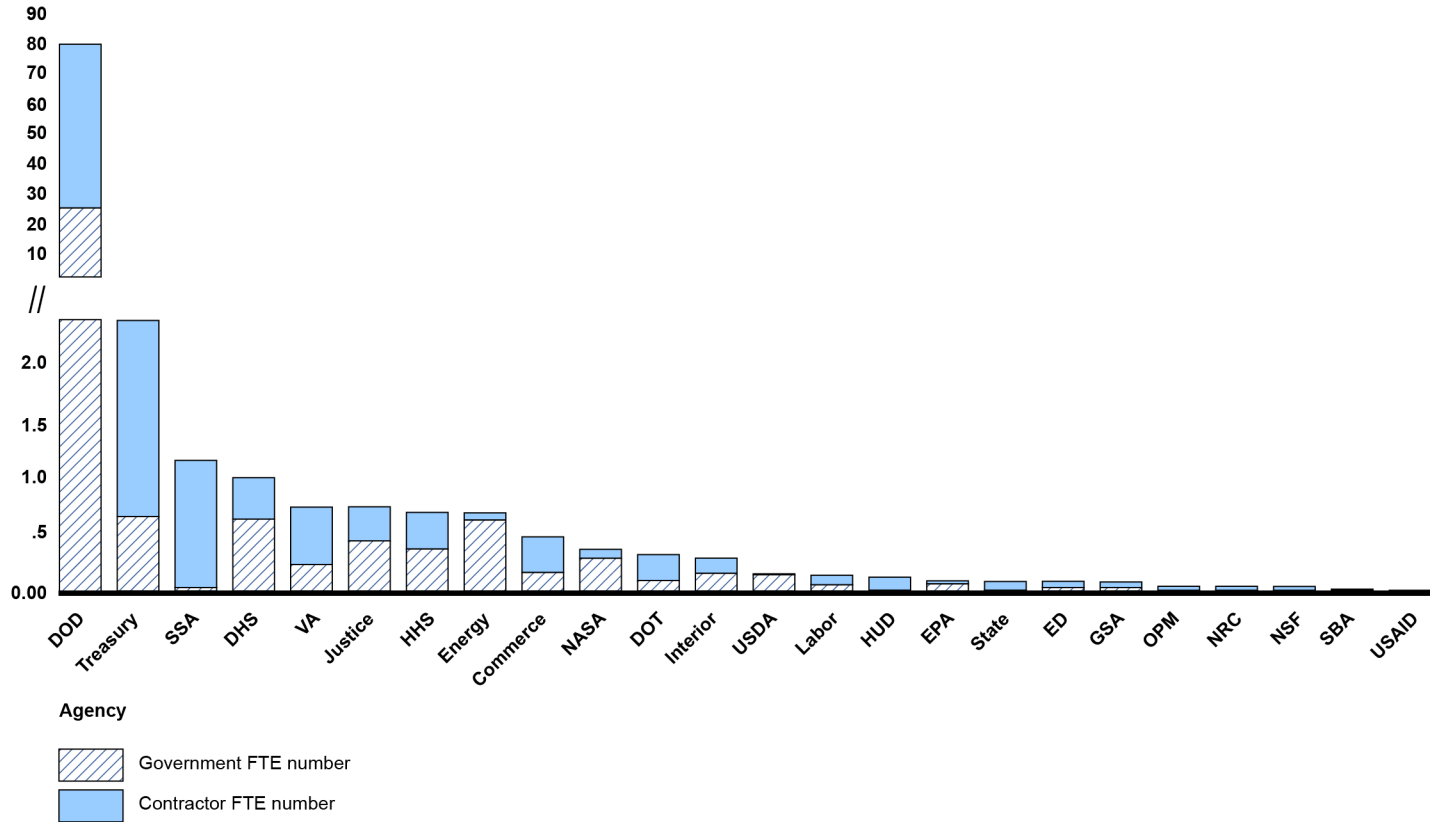
Contractors also play a prominent role in securing information and information systems for federal agencies. In fiscal year 2012, OMB reported that contractor employees accounted for 33 percent of all IT security personnel at the 24 Chief Financial Officers Act agencies. Figure 1 depicts the total number of reported IT security personnel by agency.

---

<sup>10</sup>OMB, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act*, M-14-04 (Washington, D.C.: Nov. 18, 2013).

**Figure 1: Total IT Security Personnel Reported by Agencies for Fiscal Year 2012**

IT security full time equivalents (FTEs) (in thousands)



Source: : Whitehouse.gov Fiscal Year 2012 FISMA report. | GAO-14-612

While contractor personnel who operate systems and provide services to federal agencies can provide significant benefits, they, as with government employees, can also introduce risks to agency information and systems such as the unauthorized access, use, disclosure, and modification of federal data. Specifically, contractor employees who have access to agency data and technology can introduce risks that can degrade or diminish the confidentiality, integrity, and availability of agency systems or data.

We have previously reported that agencies have identified contractor related risks to federal systems and information.<sup>11</sup> This information is summarized in table 2.

**Table 2: Examples of Risks to Federal Systems and Data from Contractors**

Category of risk	Description
People	Unauthorized contractor personnel having physical access to agency IT resources (including systems, facilities, and data).
	Unauthorized contractor personnel having electronic access to agency IT resources (including systems and data).
	Increased use of foreign nationals by contractors.
	Contractors who may not receive appropriate, periodic background investigations.
	Inadequate segregation of duties (e.g., software developer is the same individual who puts the software into production).
Policies and procedures	Failure by contractors to follow agency IT security requirements.
	Possible disclosure of agency-sensitive information to unauthorized individuals or entities.
	Lack of effective compliance monitoring of contractors performing work off site.
	Contractors may have ineffective patch management processes.
Technology	Incorporation of unauthorized features in customized application software. For example, a third-party software developer could incorporate “back doors,” spyware, or malicious code into customized application software that could expose agency IT resources to unauthorized loss, damage, modification, or disclosure of data.
	Encryption technology may not meet federal standards.
	Intentional or unintentional introduction of viruses and worms.

Source: GAO analysis of federal agencies' survey response data. | GAO-05-362

Federal agencies have reported increasing numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. Recent national security events involving the unauthorized disclosure of classified federal information have involved contractors and contractor employees. For example, in May 2012, the Federal Retirement Thrift Investment

<sup>11</sup>GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, [GAO-05-362](#) (Washington, D.C.: Apr. 22, 2005).

---

Board reported a sophisticated cyber attack on the computer of a contractor that provided services to the Thrift Savings Plan. As a result of the attack, personally identifiable information<sup>12</sup> associated with approximately 123,000 plan participants was accessed. According to the Board, the information included 43,587 individuals' names, addresses, and Social Security numbers; and 79,614 individuals' Social Security numbers and other related information. Additionally in 2013, it was reported<sup>13</sup> that a National Security Agency contractor employee had released a large amount of classified National Security Agency surveillance program data.

---

Federal Laws, Regulations, and Guidance Provide a Framework for Protecting the Privacy and Security of Information and Systems

Federal laws require agencies to protect the privacy and security of federal data and information systems. To help protect against threats to federal systems, FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, including those operated by contractors on behalf of the agency.<sup>14</sup> It requires each agency to develop, document, and implement an information security program that includes the following components:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- policies and procedures that are (1) based on risk assessments, (2) cost-effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;

---

<sup>12</sup>Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date, and place of birth, Social Security number, or other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

<sup>13</sup>*The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Processes*, Opening Statement of Subcommittee Chairman Peter T. King, before the Subcommittee on Counterterrorism and Intelligence of the H. Comm. on Homeland Security, 112th Cong. (Nov. 13, 2013).

<sup>14</sup>44 U.S.C. § 3541 – 3549, 15 U.S.C. § 278g-3.

- 
- subordinate plans for providing adequate information security for networks, facilities, and systems or group of information systems, as appropriate;
  - security awareness training to inform personnel, including contractors, of information security risks and of their responsibilities in complying with agency policies and procedures designed to reduce these risks, as well as training personnel with significant security responsibilities for information security;
  - periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of information systems;
  - a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
  - procedures for detecting, reporting, and responding to security incidents; and
  - plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Under FISMA, each agency CIO has the responsibility to ensure that agency information and information systems, including those operated by contractors, are being protected under the agency's information security program. In addition, OMB's annual FISMA reporting instructions require agencies to develop policies and procedures for agency officials to follow when performing oversight of the implementation of security and privacy controls by contractors.

FISMA requires each agency to have an annual independent evaluation of its information security program and practices, including controls testing and compliance assessment. OMB guidance specifically requires each agency inspector general, or other independent auditor, to perform the evaluation, including the effectiveness of the agency's contractor oversight. Additionally, inspectors general are to evaluate agency efforts in providing oversight of contractor employees who have privileged access to federal data and information systems.

In addition to establishing responsibilities for agencies, FISMA assigns specific information security responsibilities to OMB and NIST:

- 
- OMB is to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies. It is also responsible for reviewing, at least annually, and approving or disapproving agency information security programs. Further, OMB is to report annually to Congress on the implementation of FISMA by the agencies.
  - NIST's responsibilities include developing security standards and guidelines for agencies (other than for national security systems) that include standards for categorizing information and information systems according to ranges of risk levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.

The Privacy Act of 1974<sup>15</sup> limits how federal agencies collect, disclose, or use personal information. Under this act, agencies are to, among other things, establish appropriate safeguards to ensure the security and confidentiality of personal information maintained in a system of records<sup>16</sup> and protect it against anticipated security or integrity threats or hazards. The Privacy Act's requirements also apply to government contractors and contractor employees who have access to or maintain agency systems of records that contain personally identifiable information. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public through a system-of-records notice in the Federal Register which includes the system safeguards for the security and confidentiality of personal information.

The E-Government Act of 2002<sup>17</sup> strives to enhance the protection of personal information in government information systems or information collections by requiring that agencies conduct a privacy impact assessment (PIA)—an analysis of how personal information is collected, stored, shared, and managed in a federal system. The assessment helps inform the selection of controls that are intended to protect a system, including contractor-operated systems. Among other requirements,

---

<sup>15</sup>5 U.S.C. § 552a.

<sup>16</sup>A system of records is a collection of information about individuals under control of an agency from which information is retrieved by the name of an individual or other identifier.

<sup>17</sup>Pub. L. No. 107-347 § 208 (Dec. 17, 2002); 44 U.S.C. § 3501 note.

---

agencies must conduct PIAs before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form. In conducting PIAs, agencies are to ensure that the handling of the information conforms to applicable privacy legal requirements, determine risks, and examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.<sup>18</sup>

---

### Agency Assessments of Contractor-Operated Systems are Designed to Ensure that Federal Requirements are Met

To ensure that contractor-operated systems meet federal information security and privacy requirements, the Federal Acquisition Regulation<sup>19</sup> (FAR) requires that agency acquisition planning for IT comply with the information technology security requirements in FISMA, OMB's implementing policies including Appendix III of OMB Circular A-130, and NIST guidance and standards. The FAR addresses application of the Privacy Act to contractors at subpart 24.1, Protection of Individual Privacy.

NIST Special Publications 800-53 and 800-53A guide agencies in selecting security and privacy controls for systems and assessing them to ensure that the selected controls are in place and functioning as expected.<sup>20</sup> Additional NIST special publications on IT security services and risk management (Special Publications 800-35 and 800-37) identify several key activities important to contractor oversight for assessing the security and privacy controls of information systems. The key activities and the steps included in each are shown in table 3.

---

<sup>18</sup>OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

<sup>19</sup>The FAR establishes uniform policies and procedures for acquisition of supplies and services by executive agencies. The FAR and agency supplements are codified in title 48 of the *Code of Federal Regulations*. As relevant here, the FAR's acquisition planning requirements for IT security are at 48 C.F.R. § 7.103(w). See also, FAR § 7.105(b)(16)(*Government-furnished information*) and (18)(*Security considerations*).

<sup>20</sup>NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, (Gaithersburg, MD: Apr. 2013) and NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, (Gaithersburg, MD: Jun. 2010).

**Table 3: System Oversight Activities and Key Steps from NIST Special Publications 800-35 and 800-37**

Oversight Activity	Key Steps
Establish security and privacy requirements	<ul style="list-style-type: none"> <li>Communicate requirements to contractors. To ensure that agencies can hold contractors accountable, it is important to establish security requirements with external parties in formal contracts. The information security and privacy requirements for a system should be communicated in the contract explicitly or by reference and the FAR states that agency planners should ensure that information security and privacy requirements are addressed. To ensure that requirements are communicated to contractors, agencies must include information security and privacy language in contracts in sufficient detail to ensure that requirements are communicated effectively.</li> <li>Select and document security and privacy controls. Agencies should formally document in a system security plan, the (a) security and privacy requirements that federal employees and contractors must adhere to and (b) a description of controls in place for meeting those requirements. The security plan also includes and refers to other required security and privacy documentation, such as a PIA.</li> </ul>
Planning for control assessment	<ul style="list-style-type: none"> <li>Select an independent assessor. Agencies should ensure that an assessor is identified and selected to be responsible for conducting the security control assessment. For systems with a moderate or high impact level, an independent assessor capable of conducting an impartial assessment of security controls should be used.</li> <li>Develop a test plan. Agencies should document within a test plan which controls will be tested and selecting the appropriate assessment procedures for the system.</li> </ul>
Conducting the assessment	<ul style="list-style-type: none"> <li>Execute the test plan. Agencies should ensure that the test plan is appropriately executed and that any controls that do not satisfy the assessment criteria are documented.</li> <li>Recommend remediation actions. The final results of the assessment should be documented in the security assessment report, which includes recommended remediation actions for issues identified during testing.</li> </ul>
Reviewing the assessment results	<ul style="list-style-type: none"> <li>Review assessment results. Agency officials should review the results of the assessment and determine if the findings require investigation or remedial action.</li> <li>Develop plan of action and milestones. If remedial actions are determined to be necessary, they should be captured in a plan of action and milestones (POA&amp;M), which records the issue, estimated dates for resolution, resources assigned, and any other information necessary to prioritize the remediation.</li> </ul>

Source: GAO analysis of NIST special publications 800-35, Guide to Information Technology Security Services and 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. | GAO-14-612

### GAO has Previously Reported on Agencies' Oversight of Contractors

In April 2005,<sup>21</sup> we reported on federal agencies' implementation of FISMA requirements and their oversight of contractors and others with privileged access to federal data and systems. We determined that, although most agencies reported having written policies that addressed information security for contractor-provided IT services and systems, few had established specific policies for overseeing the information security practices of contractors and contractor employees to ensure compliance

<sup>21</sup>[GAO-05-362](#).



---

with contract requirements and agency information security policies. We concluded that, without specific oversight policies establishing when and how agencies will review contractor-operated systems, officials responsible for the systems may not be taking sufficient action to ensure that security requirements are being met. We recommended, among other things, that the Director of OMB ensure that federal agencies develop policies for ensuring the information security of contractors and other users with privileged access to federal data. Subsequently OMB modified its instructions to better ensure that federal agencies develop policies for ensuring the information security provided by contractor employees.

---

## Agency Oversight of Contractor-Operated Systems Was Not Always Consistent

Under FISMA, each agency CIO has the responsibility to ensure that agency information and information systems, including those operated by contractors, are being protected under the agency's information security program. In addition, OMB's annual FISMA reporting instructions require agencies to develop policies and procedures for agency officials to follow when performing oversight of the implementation of security and privacy controls by contractors. CIO oversight of the agency's information security program provides agency officials assurance that they are protecting sensitive agency information. According to NIST, assessment of security and privacy controls is a key element of security program oversight.

While the six agencies we reviewed generally established security and privacy requirements for contractors to follow and prepared for assessments to determine the effectiveness of contractor implementation of controls, five of the six were inconsistent in overseeing the execution and review of those assessments. Table 4 details the degree of implementation of oversight activities for the selected systems at each agency.

**Table 4: GAO Evaluation of Agency Oversight of Selected Contractor-Operated Systems**

		Establish security and privacy requirements		Plan assessment		Conduct assessment		Review assessment	
		Communicate requirements to contractors	Select and document controls	Select independent assessor	Develop test plan	Execute test plan	Recommend remediation actions	Review results	Develop plan of action and milestones
DOE	System 1	●	●	●	○	○	●	○	●
	System 2	●	●	●	●	●	●	●	●
DHS	System 1	●	●	●	●	●	●	●	●
	System 2	●	●	●	●	●	●	●	●
State	System 1	○	●	○	●	◐	●	◐	◐
	System 2	●	●	○	●	◐	●	●	◐
DOT	System 1	○	●	●	●	◐	●	●	●
	System 2	●	●	●	●	◐	●	◐	◐
EPA	System 1	●	●	●	●	◐	●	●	◐
	System 2	●	●	●	●	●	●	●	●
OPM	System 1	●	●	●	●	◐	●	●	●
	System 2	●	●	●	●	◐	●	●	●

Source: GAO analysis of agency data. | GAO-14-612.

● Fully Implemented ◐ Partially Implemented ○ Not Implemented

While agencies performed two of the eight key steps in all cases, most were inconsistent in performing the remaining steps for the oversight of the selected contractor-operated systems. Specifically:

- Communicate requirements to contractors.* Four of the six agencies (DOE, DHS, EPA, and OPM) communicated security and privacy requirements to contractors in contracts for the systems we reviewed. For example, a contract for one system at EPA specifically required the contractor to comply with the EPA information security policy. Two of the six agencies (DOT and State) did not always communicate security and privacy requirements to contractors in the contracts for agency systems. NIST guidance states that security requirements should be stated explicitly or by reference in contracts. However, while State’s departmental policies include references regarding contractor requirements for protecting personally identifiable information and system authorization, the contract for one system that we reviewed did not contain language that communicated these requirements. Furthermore, while the contract for one of the systems at DOT was modified to include requirements for background investigations, there was no language included that communicated

---

agency security and privacy requirements. Officials for both agencies were not able to explain why this language was not included in the contracts. Without specific security requirements in the contract, these two systems are at an increased risk that contractors may not understand the requirements that they are expected to implement or cannot be held to the security and privacy requirements during contract performance.

- *Select and document security and privacy controls.* All 12 of the systems that we reviewed documented the security and privacy controls that were expected to be implemented for the system within the system security plan. According to NIST Special Publication 800-37, system security plans are intended to provide an overview of the security requirements for the system and describe the security controls in place or planned for meeting those requirements. Each agency supported the selection of controls by documenting privacy risks and impacts to the systems we reviewed within a PIA, as called for when systems contain personally identifiable information.
- *Select an independent assessor.* Five of the six agencies ensured that assessors used for systems we reviewed were independent, as required by NIST. For moderate impact information systems and higher, such as the ones that we reviewed, NIST states that an independent third party reviewer should be used for the assessment to ensure that the review is unbiased. For example, for both systems we reviewed at OPM, the agency used a different contractor to assess the system and system officials took steps to verify that the assessor was independent. However, one agency, State, did not ensure that the assessors used for both systems we reviewed were independent. State officials allowed the contractor to select the assessor for both systems we reviewed and did not take steps to verify the assessor's independence. State officials stated that they believe it was not their responsibility to ensure the independence of the assessors for the particular systems. As a result, the agency has reduced assurance that assessments were complete and unbiased.
- *Develop a test plan.* Five of the six agencies adequately documented test plans for the assessments of the two systems we reviewed at each agency. These plans documented the controls to be tested and appropriate assessment procedures. NIST Special Publication 800-53A states that test plans are to document the objectives for the security control assessment and provide a detailed road map of how the assessors are to test the information security and privacy controls for the system. One of the six agencies (DOE) did not document

---

which controls from the system security plan were to be tested and the assessment procedures that were to be followed for one system as the officials could not locate the system test plan. DOE officials stated that the computer housing the information became corrupted and the detailed test plan could therefore not be provided.<sup>22</sup> Officials stated that, in response to our audit, they now plan to expedite the development of a test plan to be executed this year. Without a detailed test plan, agency officials have reduced assurance that the selected controls were tested and that the correct tests were executed.

- *Execute the test plan.* One of the six agencies (DHS) effectively executed the test plan for the two systems we reviewed. For both of its systems, the controls from the test plan, were effectively tested, and for areas such as background investigation and contingency plan training evidence was provided showing that all of the contractors operating the system had received an investigation or training. NIST guidance calls for agencies to ensure that the test plan is appropriately executed during the assessment process.

However, the system assessments that were performed by five of the six agencies (DOE, DOT, EPA, OPM, and State) were not always effective. For example, DOT and State did not always ensure that system assessments evaluated the extent to which background investigations had been conducted for contractor employees. Instead, the agencies relied on agency-wide testing of personnel security as a common control.<sup>23</sup> However, agency-wide testing was not comprehensive enough to identify lapses that we found regarding background investigations<sup>24</sup> for contractor personnel working on these systems. Specifically, for one of the DOT systems we reviewed,

---

<sup>22</sup>We did not assess the extent to which the agency adhered to federal and agency-specific records management requirements or why the agency did not have a backup of this information.

<sup>23</sup>Common controls are those security and privacy controls that are assessed once by an organization and whose assessment results are inheritable by one or more organizational information systems in order to reduce duplicative testing.

<sup>24</sup>As relevant here, background investigations allow federal agencies to make decisions about a person's suitability for access to federal property, information, and systems under a federal contract. Agencies evaluate the information in a completed background investigation to make a determination whether, among other things, an individual is fit to perform work for or on behalf of the government as a contractor employee.

---

department officials responsible for system testing had not evaluated whether the seven contractor employees working on the system had the required background investigation. When they did so in response to our audit, they found that three of them did not. Officials stated that they subsequently removed system access rights for the three contractor employees until their background investigations had been completed.<sup>25</sup> For the department's other selected system, DOT officials did not have evidence that 44 of 133 contractor employees had undergone a current background investigation.

For the two State systems we reviewed, department officials responsible for these systems stated that they did not believe that it was necessary for them to check whether contractor employees had undergone a background investigation. However, the system security plans for both State systems had documented the selection of background investigations as applicable security controls, therefore calling for them to be included in the scope of testing. By not testing that all contractor employees operating a system have had an appropriate background investigation completed, agency officials lack assurance that contractor employees can be trusted with access to government information and systems.

Furthermore, for 8 of the 12 systems that we reviewed, the agencies did not always ensure that system assessments accurately evaluated the extent to which contractor employees had completed contingency plan training as required. NIST guidance states that anyone with responsibilities for implementing the contingency plan should receive regular training on their role. However, DOE, DOT, EPA, OPM and State officials were unable to demonstrate that contractor employees had received the necessary training despite assessment results that stated they had. Additionally, DOT officials were unable to identify whether several staff members listed in the contingency plan of one system were federal employees or contractor personnel. Overseeing that key contractor staff had taken or completed the contingency plan training would provide increased assurance that contractor employees are familiar with their roles and responsibilities under the contingency plan.

- *Recommend remediation actions.* All 12 of the system assessments that we reviewed produced a report showing recommendations from

---

<sup>25</sup>According to DOT, those contractors have since received favorable background determinations and are working on the system again.

---

the assessor. NIST states that, since results of the security control assessment ultimately influence the content of the system security plan and the plan of action and milestones, agency officials should review the security assessment report to determine the appropriate steps required to correct weaknesses and deficiencies identified during the assessment. Furthermore, assessors' recommendations in the security assessment report are an important input into agency officials' risk-based decisions on addressing weaknesses. All 12 of the system assessments that we reviewed included recommendations to address weaknesses.

- *Review the assessment results.* Three of the six agencies (DHS, EPA, and OPM) adequately reviewed assessment results, ensuring that all of the controls selected for the systems and the evaluation methods used for the controls were included. However, three of the six agencies (DOT, DOE, and State) did not adequately review the assessment results. For one system at DOT, DOE, and State, documentation provided by agency officials showed that a thorough review had not occurred by the authorizing official. NIST states that the systems authorizing official or designated representative is to assess the current security state of the system or the common controls inherited by the system. For the system at DOT, the test evidence for the media protection and physical security controls (25 total controls) that was documented, reviewed, and accepted was from a different DOT system. DOT officials confirmed that these controls had not been sufficiently tested and that they would test them as part of their next system assessment. At DOE, officials were able to provide the executive summary of the test results but could not show that the full test results had been reviewed. Agency officials stated that the computer housing the information became corrupted and the detailed test results could not be provided.<sup>26</sup> In addition, at State, a system security control assessment did not document that 69 of the systems' controls were tested, and the assessment showed that the results were reviewed and accepted. State officials were unable to provide a reason for this lapse. Without properly reviewing the assessment results, agency officials may lack assurance that all of the controls selected for a system are properly tested.

---

<sup>26</sup>We did not assess the extent to which the agency adhered to federal and agency-specific records management requirements or why the agency did not have a backup of this information.

- 
- *Develop a plan of action and milestones for remediation of weaknesses.* Three of the six agencies (OPM, DHS, and DOE) for both systems we reviewed maintained POA&M that included all of the NIST elements, such as estimated completion dates, resource allocation and issue identification. For example, for one system we reviewed at OPM, the POA&M is maintained by agency officials using a software application that includes the elements required by NIST. However, three of the six agencies (DOT, State, and EPA) did not always complete or update POA&Ms for their contractor-operated systems. Specifically, the POA&Ms for one of the two systems we reviewed at State and DOT were missing information such as estimated completion dates and resources that were assigned to resolution. Additionally, State did not include all of the weaknesses identified in the assessment report within the POA&M for the second system we reviewed. State officials stated that those weaknesses should have been captured in the POA&M. EPA could not provide an updated POA&M for one of the two systems we reviewed. Without complete or up-to-date POA&Ms, agencies increase the risk that identified weaknesses will not be resolved in a timely fashion.

---

### Selected Agencies Have Not Developed Procedures for Overseeing the Privacy and Security of Federal Information on Contractor-Operated Systems

The responsibility for adequately mitigating risks arising from the use of contractor-operated systems remains with the agency. OMB's annual FISMA reporting instructions require agencies to develop policies for information security oversight of contractors<sup>27</sup> and the FAR, in its procedures for acquisition planning, requires agencies to ensure that information technology acquisitions comply with FISMA, OMB's implementing policies, and NIST guidance and standards.<sup>28</sup> Further, NIST SP 800-53 states that agencies should develop, document and implement a process that provides oversight to ensure that agency testing of security and privacy controls is planned and conducted consistent with organizational priorities.

A contributing reason for shortfalls identified in agency oversight of contractors was that agencies had not documented procedures to direct officials in performing such oversight activities effectively. For example,

---

<sup>27</sup>OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, (Washington, D.C.: November 2013).

<sup>28</sup>48 C.F.R. § 7.103(w).

---

system officials for one system at DOT that accepted assessment results for 25 controls from the wrong system; the department did not have procedures in place to direct officials on how to effectively review such test results.

According to the Office of the CIO officials we interviewed from each of the six selected agencies, all information security and privacy policies and procedures of each agency apply to their federal employees and systems as well as to contractors, contractor employees, and contractor-operated systems, and the system assessment process is intended to provide assurance that these policies and procedures are being implemented. However, as described in the previous section, we found inconsistencies in the oversight of contractor-operated systems at five of the six agencies; none of the agencies had procedures in place to direct officials in how to conduct such oversight. Such inconsistencies may have been mitigated if procedures had been created, documented and implemented. For example, agency officials reviewing system assessment results could refer to a procedure outlining the necessary actions for an effective review of an assessment conducted by contractors. As a result, agency officials have less assurance that oversight activities are being performed consistently and effectively over all of their contractor-operated systems and weaknesses may go undetected and unresolved, such as having contractor employees operate a system without undergoing a background investigation.

---

## Government-wide Guidance for Contractor-Operated Systems Assists Agencies, but OMB Guidance Needs Clarification

In fulfilling its responsibilities to develop guidance and oversee the implementation of FISMA, OMB has issued guidance for agencies to ensure that contractors and contractor employees meet agency information security and privacy requirements. Specifically, OMB issues annual FISMA reporting instructions to guide agencies as they report on their security requirements. The instructions state that agencies are responsible for ensuring that systems operated by contractors meet FISMA information security requirements. The OMB instructions also state that systems operated by contractors are to be reported as part of the agency's system inventory, tested on an annual basis, and reviewed appropriately. OMB collects the information from agencies on their implementation of FISMA, and then provides a summary of the data in an annual report to Congress.

Further, OMB has developed guidance over several years to assist agencies in assessing their contractors' performance. The guidance ranges from providing agencies with overarching requirements for



managing contractors to requiring agency officials with acquisition and procurement responsibilities to take specific actions. Examples of OMB guidance for agencies that address contractor management are shown in table 5.

**Table 5: OMB Memoranda on Contractor Oversight**

<b>Memorandum</b>	<b>Description</b>
M-09-25—Improving Government Acquisition (July 2009)	Provides guidance to agencies on reviewing existing contracts and acquisition practices.
M-09-26—Managing the Multi-Sector Workforce (July 2009)	Requires agencies to develop and implement policies, practices, and tools for managing the multi-sector workforce, and ensure that they are not over-relying on contractors.
Memorandum on Improving the Use of Contractor Performance Information (July 2009)	Provides guidance for improving the use of contractor performance information.
Memorandum on Improving Contractor Past Performance Assessments (January 2011)	Summarizes OMB’s review of contractor past performance assessments and recommends additional steps and strategies for improving the collection of past performance information.
Memorandum on Improving the Collection and Use of Information about Contractor Performance and Integrity (March 2013)	Provides guidance for improving the collection and use of information about contractor performance and integrity, establishes a baseline for reporting compliance, sets performance targets to monitor and measure reporting compliance and includes information on training the workforce.

Source: GAO analysis of OMB memoranda. | GAO-14-612

OMB has also tasked DHS with certain responsibilities assisting government-wide efforts to provide adequate, risk based, and cost-effective cybersecurity.<sup>29</sup> OMB and DHS have met with agency CIOs, chief information security officers, and other agency officials to discuss and assist in developing focused strategies for improving their agency’s cybersecurity posture. OMB officials from the Office of E-Government and Information Technology stated that agency contractor oversight for contractor-operated systems is discussed as needed at these meetings and that assisting agencies in implementing OMB guidance and

<sup>29</sup>OMB memorandum M-10-28 stated that DHS was to exercise primary responsibility within the executive branch for the operational aspects of cybersecurity for federal information systems that fall within the scope of FISMA. OMB, *Memorandum M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (Washington, D.C.: July 6, 2010).

---

instructions provides greater protections for all of an agency's systems, including contractor-operated systems. OMB officials from the same office stated that these meetings allow them to conduct outreach and education to assist agencies in understanding their guidance as necessary.

---

### OMB Guidance is Not Clear on When Systems Should Be Identified and Reported as Contractor-Operated

OMB guidance to agencies for categorizing and reporting contractor-operated systems does not clearly define what a contractor-operated system is and consequently, agencies are interpreting the guidance differently. FISMA assigns OMB responsibilities to develop and oversee the implementation of policies, principles, standards, and guidelines on information security in federal agencies. Guidance provided as part of OMB's annual FISMA reporting instructions identifies several types of contractor relationships an agency may have in using a contractor for a system.<sup>30</sup> However, it does not specify which agency systems that have contractor relationships should be categorized as contractor-operated. We and the inspectors general have found that not all agencies are interpreting this guidance in the same manner. Specifically, two of the six agencies we reviewed did not report all of their systems that are operated by contractors on their behalf as "contractor-operated" in their FISMA submissions. For example, CIO officials from the State Department stated that the number of contractor-operated systems the department reported as part of its 2012 FISMA submission did not include all systems that are operated by contractors. Rather, officials stated that the department only reported those systems that are both owned and operated by contractors by this label and identifies systems that are government-owned as "agency-operated" even when contractors operate the system on behalf of the department. Conversely, DHS officials stated that it reports systems as "contractor operated" only when they are government-owned but operated by contractors. DHS systems that are both owned and operated by contractors are designated by a third category known as an "external information system." Those systems are not included in either the list of department's agency-operated systems or contractor-operated systems.

Additionally, in their fiscal year 2012 annual FISMA reports, inspectors general from 9 of the 24 major agencies found data reliability issues with

---

<sup>30</sup>The agency contractor relationship categories are defined by OMB as (1) service providers; (2) contractor support; (3) government-owned, contractor-operated facilities; (4) laboratories and research centers; and (5) management and operating contracts.

---

their agencies' categorization of contractor-operated systems.<sup>31</sup> For example, DOT's Inspector General reported that 24 of the Department's 60 information systems were owned and operated by a contractor, but only 4 were categorized as being contractor-operated by the department.

OMB officials from the Office of E-Government and Information Technology stated that they believe the current guidance is sufficient to assist agencies in categorizing and reporting contractor-operated systems. OMB officials stated that, while they would not be able to identify all of the types of relationships that agencies have with contractors, agencies can refer to the guidance contained within the FISMA reporting instructions and its outline of five different categories of relationships that agencies may have with contractors operating systems or processing information on the agencies' behalf.

Nevertheless, the inconsistent implementation of OMB's reporting guidance by agencies in reporting the number of contractor-operated systems demonstrates that existing outreach and education efforts during face-to-face meetings with agency information security officials are not always resulting in accurate reporting of agencies' reliance on contractors to operate systems and process government information on their behalf. Consequently, agencies are not reporting all of their contractor-operated systems in their FISMA submissions, the information is not complete enough to provide OMB with an accurate representation of the number of contractor-operated systems within the government, and OMB's report to Congress on the implementation of FISMA is not complete. Without complete information about contractor-operated systems, OMB and DHS may limit their ability to assist agencies in improving their cybersecurity postures and Congress will not have complete information on the implementation of FISMA.

---

<sup>31</sup>The agencies were the Departments of Agriculture, Defense, Health and Human Services, Interior, Transportation, Veterans Affairs, the Office of Personnel Management, the Social Security Administration, and the U.S. Agency for International Development.

---

## NIST and GSA Provide Guidance to Agencies for Addressing Security and Privacy Requirements for Contractor-Operated Systems

FISMA requires NIST to develop security standards and guidelines for agencies (other than national security systems), including when information and information systems are used or operated by a federal contractor on behalf of an agency. OMB Circular A-130 states that GSA should provide agencies with security guidance when acquiring information technology products or services.

To meet its FISMA requirements, NIST has issued guidance for agencies to follow in overseeing contractors as they operate, use, and access government information and information systems. It has produced numerous information security standards and guidelines and has updated existing information security publications to assist agencies in developing and implementing an information security program that manages risks, including those risks incurred through the use of contractors. For example, in April 2013, NIST released its fourth update of a key federal government computer security control guide, Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations, which contains an external service providers section that has requirements for agencies to ensure that contractors meet the same requirements that agencies adhere to and recommends that agencies incorporate oversight controls such as establishing personnel security requirements, requiring third-party providers to notify the agency of personnel transfers, and monitoring provider compliance. Further, the guide includes an appendix on identifying and implementing controls for protecting privacy within an organization, including contractors.

Further, NIST officials stated that the risks incurred from utilizing contractors should be addressed by incorporating the risk management framework as part of the terms and conditions of the contract and that agencies can specify the security controls for which the contractor must implement and require appropriate evidence to demonstrate that they effectively implemented the specified controls. The risk management framework, specified in NIST Special Publication 800-37, provides a process that integrates information security and risk management activities into the system development life cycle.

GSA, in meeting its responsibilities under OMB Circular A-130 issued guidance, templates, and established pre-negotiated contracts for agencies using contractors to maintain agency information and systems.

---

GSA has also published an acquisition manual to assist agencies when they choose to create their own contracts.<sup>32</sup>

Additionally, GSA has negotiated contracts for products and services to assist agencies transitioning to cloud computing services. Cloud computing services are being managed through FedRAMP, a government-wide program to provide joint authorization and continuous security monitoring services for all federal agencies. GSA creates standardized FedRAMP templates for contract language and security assessments, among other things, and sample service level agreements for use in cloud service acquisitions.

---

## Conclusions

The six agencies reviewed made efforts to assess the implementation of security and privacy controls for selected contractor-operated systems. The agencies generally had established security and privacy requirements for contractors to follow and prepared for assessments to determine the effectiveness of contractor implementation of controls. However, oversight of the execution and review of assessments of contractor-operated systems was not consistent at five of the six agencies we reviewed. Specifically, agencies did not always prepare, execute, and review assessments of their contractor-operated systems. A contributing reason for these shortfalls is that agencies had not documented procedures for officials to follow in order to perform such oversight of contractors effectively. Until these agencies develop, document and implement specific procedures for overseeing contractors, they will have reduced assurance that the contractors are adequately securing and protecting agency information, including of the extent to which contractors have undergone background investigations.

OMB, NIST, and GSA have provided agencies guidance to assist in implementing privacy and security controls for contractor-operated systems. In addition, OMB and DHS are taking actions to assist agencies in planning to improve their cybersecurity posture. However, the lack of clear instructions to agencies for reporting contractor-operated systems has contributed to incomplete information regarding the number of contractor-operated systems within the government. Without complete information, OMB and DHS assistance to agencies for improving their

---

<sup>32</sup>*General Services Administration Acquisition Manual.*

---

cybersecurity postures is limited and Congress will not have complete information on the implementation of FISMA.

---

## Recommendations for Executive Action

To ensure that the privacy and security controls of contractor-operated systems are being properly overseen, we are making 15 recommendations to five selected agencies.

We recommend that the Secretary of Energy develop, document, and implement oversight procedures for ensuring that, for each contractor-operated system:

- a system test plan is developed,
- a system test is fully executed, and
- test results are reviewed by agency officials.

We recommend that the Secretary of State develop, document, and implement oversight procedures for ensuring that, for each contractor-operated system:

- security and privacy requirements are communicated to contractors,
- an independent assessor is selected to assess the system,
- a system test is fully executed,
- test results are reviewed by agency officials, and
- plans of action and milestones with estimated completion dates and resources assigned for resolution are maintained.

We recommend that the Secretary of Transportation develop, document, and implement oversight procedures for ensuring that, for each contractor-operated system:

- security and privacy requirements are communicated to contractors,
- a system test is fully executed,
- test results are reviewed by agency officials, and
- plans of action and milestones with estimated completion dates and resources assigned to resolution are maintained.

We recommend that the Administrator of the Environmental Protection Agency develop, document, and implement oversight procedures for ensuring that, for each contractor-operated system:

- a system test is fully executed and
- plans of action and milestones with estimated completion dates and resources assigned for resolution are maintained.

---

---

## Agency Comments and Our Evaluation

We recommend that the Director of the Office of Personnel Management develop, document, and implement oversight procedures for ensuring that a system test is fully executed for each contractor-operated system.

To be able to effectively assist agencies with their contractor oversight programs, we recommend that the Director of the Office of Management and Budget, in collaboration with the Secretary of Homeland Security develop and clarify reporting guidance to agencies for annually reporting the number of contractor-operated systems.

We received comments on a draft of this report from five of the six agencies to which we made recommendations. We requested comments from the Office of Management and Budget, but none were provided. The Departments of Energy, State, and Transportation, the Environmental Protection Agency and the Office of Personnel Management, generally agreed with our recommendations. A summary of their comments and our responses, where appropriate, are provided below.

- In written comments, the Chief Information Officer for DOE stated that the department is working to align with the recommendations. For the one system where the department could not produce the test plan or show evidence that the plan had been executed, the department has targeted that system for a new security test and evaluation. DOE's full comments are provided in appendix II.
- In written comments, the acting Comptroller of the Department of State stated that the department agrees with our recommendations and is planning to develop, document, and implement oversight procedures for each contractor-operated, contractor-owned system. Additionally, he stated that department entities will seek to ensure the privacy and security controls of all contractor-operated systems. State's comments are provided in appendix III.
- The Deputy Director of Audit Relations from DOT stated via e-mail that the department agrees to consider our recommendations. We continue to believe that the department needs to develop, document, and implement oversight procedures for each contractor-operated system.
- In written comments, EPA's Acting Principle Deputy Assistant Administrator and Acting Deputy Chief Information Officer concurred with our recommendations. In addition, EPA provided information related to our draft finding that a plan of action and milestones for a

---

system had not been updated by EPA since 2011. As a result of this information, we have modified the report and recommendation as appropriate. EPA's comments are provided in appendix IV.

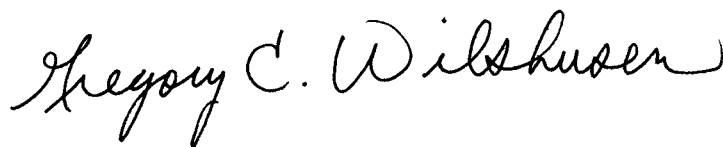
- In written comments, the OPM Chief Information Officer concurred with our recommendation and stated that OPM will review its policies and procedures to further enhance OPM's oversight of contractor-operated systems. OPM's comments are provided in appendix V.

In addition, the three agencies covered by our review that did not receive recommendations also reviewed our draft. In written comments DHS's Director of the Departmental GAO-OIG Liaison Office stated that although the Department did not receive a recommendation in this report, it will collaborate with OMB to update the FISMA guidance in support of our recommendation to OMB. DHS's comments are provided in appendix VI. The other two agencies—GSA and NIST—responded via e-mail that they had no comment on the report through a representative of GSA's GAO/IG Audit Response Division and a representative of NIST's Management and Organization Division. We also received technical comments from the Department of State, which we addressed as appropriate.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Administrators of the Environmental Protection Agency and the General Services Administration, the Directors of the Office of Management and Budget and the Office of Personnel Management, the Secretaries of Energy, Homeland Security, State, and Transportation, and other interested parties. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VII.



Gregory C. Wilshusen  
Director, Information Security Issues



---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to assess the extent to which (1) selected agencies oversee the security and privacy controls for systems that are operated by contractors on their behalf and (2) executive branch agencies with government wide guidance and oversight responsibilities have taken steps to assist agencies in ensuring implementation of information security and privacy controls by contractors.

For our first objective, we selected a non-generalizable sample of six Chief Financial Officers Act agencies. The six agencies selected were the Departments of Energy, Homeland Security, State, and Transportation; the Environmental Protection Agency; and the Office of Personnel Management. We selected these 6 agencies based on the number of contractor operated systems reported by the 24 Chief Financial Officer Act agencies from fiscal year 2011 Federal Information Security Management Act (FISMA) data. Specifically, we identified the eight agencies with the largest reported number of contractor-operated systems as high, the next eight agencies as medium, and the last eight agencies as low. We then selected the top two from the high, medium, and low groupings in order to review agencies that had a reported range in the number of contractor operated systems.

To gain insight into the six agencies' practices for protecting the security and privacy of information and systems, we interviewed officials and reviewed documentation regarding their policies and procedures for overseeing contractor privacy and security practices, including reviewing each agency's policies and procedures for identifying risks and vulnerabilities, providing security awareness training to personnel with significant information security responsibilities, developing plans of action and milestones, developing incident response plans, and testing of system security controls. We conducted interviews with officials from each agency's Office of the Chief Information Officer, Privacy Office, procurement office, as well as system owners to understand how they oversee the implementation of the Federal Acquisition Regulation (FAR), FISMA, and Privacy Act requirements, relevant OMB policies, National Institute of Standards and Technology (NIST) guidance, and agency-wide and system-level policies and procedures.

To understand how well agencies' were overseeing the implementation of agency requirements by contractors, we reviewed oversight efforts by agencies at the system level. We selected two systems at each agency using a non-generalizable random sample from a list of agency provided contractor-operated systems that were identified as having personally identifiable information and as either government-owned and contractor-

operated and contractor-owned and contractor-operated. We examined whether the agencies for each selected system implemented oversight over key elements of federal requirements and guidance such as the FAR; FISMA; the Privacy Act, and NIST and Office of Management and Budget (OMB) guidance. The key elements were communicating requirements to contractors, selecting and documenting security controls, selecting an independent assessor, developing a test plan, executing the test plan, recommending remediation actions, reviewing results, and developing a plan of action and milestones. We also assessed whether agency officials at selected information systems implemented policies and procedures set forth by the agency, including contractor oversight activities performed by the responsible agency official.

For our second objective, we reviewed requirements and guidance provided by OMB, NIST, and the General Services Administration (GSA) to agencies used to assist them in conducting contractor oversight. We interviewed DHS, GSA, OMB, and NIST officials regarding the policies and procedures for overseeing contractor privacy and security, and the activities taken to provide assistance to agencies regarding oversight of contractor-operated systems. We analyzed agency responses to OMB and DHS guidance regarding contractor-operated systems. We also reviewed inspectors general FISMA reports to assess agencies progress in meeting FISMA reporting requirements related to contractor security, including the reliability of the reporting of contractor-operated systems by agencies. We also interviewed officials of inspectors' general of the agencies we reviewed for the first objective to discuss how the agency's are reporting their inventory of systems.

We conducted this performance audit from February 2013 to July 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Appendix II: Comments from the Department of Energy



Department of Energy  
Washington, DC 20585

July 10, 2014

Gregory C. Wilshusen  
Director, Information Security Issues  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, D.C. 20548

Mr. Wilshusen:

The Department of Energy (DOE) Office of the Chief Information Officer (OCIO) appreciates the opportunity to provide comments to the Government Accountability Office's (GAO) Draft Report, *Information Security: Agencies Need to Improve Oversight of Contractor Controls* (GAO-14-612).

The *Federal Information Security Management Act (FISMA) of 2002* requires risk and vulnerability assessments and continuous monitoring on a periodic basis and, at a minimum, annually. The National Institute of Standards and Technology Special Publication (SP) 800-137, *Information Security Continuous Monitoring*, and SP 800-39, *Guidelines for a Risk Management Framework*, serve as DOE's guide for risk management and continuous monitoring. Furthermore, improving oversight of contractor controls is an important focus for DOE.

The Department continues to make significant progress in strengthening its oversight capabilities with regard to contractor controls through the implementation of DOE Order 205.1B – Cyber Security Program (CSP), which states: "DOE Oversight is conducted through Assurance Systems that monitor the risk evaluation and protection processes at each level in the organization. CSP emphasizes risk management rather than a system-level 'controls-compliance' approach. Through the Risk Management Approach (RMA), the Department effectively and efficiently meets its obligations under FISMA in a manner that improves, rather than impedes the fulfillment of the Department's statutory mission." To ensure the enforcement of DOE Order 205.1B, the CSP through DOE's RMA has established line management accountability for ensuring protection of information and information systems through the Department's Program Offices to their program elements.

In addition, the RMA recognizes the Department's federated government-owned/contractor operated environment and appropriately integrates cyber security governance, accountability and reporting into management and work practices at all levels of the Department. Furthermore, the Department has specifically implemented an oversight policy, DOE Order 226.1B – *Implementation of the Department Oversight Policy*. This order addresses DOE contracts for the management and operation of DOE-owned or DOE-leased facilities.



Printed with soy ink on recycled paper

DOE is confident that the policies and procedures that are in place, including the Program Cyber Security Plan—which is required at all DOE offices and field sites—ensures the oversight necessary to effectively implement security and privacy requirements, assess implementation, and take appropriate corrective actions.

**Management Response:**

- We have reviewed the subject GAO report and have no comments regarding technical accuracy. Of the two DOE systems reviewed, only one, “System 1”, was identified as having deficiencies in three out of eight areas. As stated in the GAO report, DOE could not produce the test plan or show evidence that the plan was executed. However, it was noted that the system owners were fully compliant on Recommended Remediation Actions. My staff has verified that the Plan of Action and Milestones (POA&Ms) developed for System 1 was reviewed and approved by the appropriate Program Office sub-element;
- “System 1” has been targeted for a new Security Test and Evaluation (ST&E). The plan and results will be filed in the official compliant Legacy Management Records Keeping System on September 30, 2014. Upon filing of the final ST&E Plan and results, DOE will consider this recommendation closed.

The Department has made significant efforts to strengthen our oversight responsibilities through DOE policies and contractor requirements. DOE’s RMA and accountability through Program Offices continue to be effective in conducting required tests, and taking remedial actions through the POA&M submission and Program Office sub-element review process.

Again, I thank you for the opportunity to review this report. I can assure you that DOE is working to align with your recommendations. If you have any questions, please feel free to contact me at 202-586-0166.

Sincerely,



Robert F. Brese  
Chief Information Officer

# Appendix III: Comments from the Department of State



United States Department of State  
*Comptroller*  
P.O. Box 150008  
Charleston, SC 29415-5008

JUL 08 2014

Dr. Loren Yager  
Managing Director  
International Affairs and Trade  
Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20548-0001


Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "INFORMATION SECURITY: Agencies Need to Improve Oversight of Contractor Controls" GAO Job Code 311303.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Gary Galloway, Deputy Director, Bureau of Information Resource Management, Office of Information Assurance at (202) 634-3047.

Sincerely,

  
Christopher H. Flaggs, Acting

Enclosure:

As stated.

cc: GAO – Gregory C. Wilshusen  
IRM – Steven C. Taylor  
State/OIG – Norman Brown

UNCLASSIFIED

**Department of State Comments on GAO Draft Report**

**Agencies Need to Improve Oversight of Contractor Controls**  
**(GAO-14-612, GAO Code 311303)**

The Department of State welcomes the opportunity to comment on the draft report *INFORMATION SECURITY: Agencies Need to Improve Oversight of Contractor Controls*.

After review, the Department of State agrees with GAO and is planning to develop, document, and implement oversight procedures to ensure that for each contractor-operated, contractor-owned system:

- security and privacy requirements are communicated to contractors;
- an independent assessor is selected to assess each system;
- a system test is fully executed;
- test results are reviewed by agency officials; and
- plans of action and milestones are maintained with estimated completion dates and resources are assigned for resolution.

In addition, Department entities will seek to ensure the privacy and security controls of all contractor-operated systems.

Thank you again for the opportunity to respond to the GAO draft report and for the courtesies extended by your staff in the conduct of this review.

# Appendix IV: Comments from the Environmental Protection Agency



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY  
WASHINGTON, D.C. 20460

OFFICE OF  
ENVIRONMENTAL INFORMATION

Mr. Nicholas Marinos,  
Assistant Director  
Information Security Issues  
U.S. Government Accountability Office  
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review and comment of GAO's draft report, *Information Security: Agencies Need to Improve Oversight of Contractor Controls* (GAO-14-612). The purpose of this letter is to provide the U.S. Environmental Protection Agency's (EPA) response to your recommendations addressed to EPA.

GAO recommends that EPA develop, document and implement oversight procedures that, for each contractor-operating system: (1) a system test is fully executed and (2) plans of action and milestones are maintained with estimated completion dates and resources assigned for resolution.

EPA concurs with the GAO recommendations but has one clarification. EPA will work to improve how we conduct and execute the test plan, and have already made much progress. We will also resolve any outstanding plans of action and milestones associated with the system that was reviewed by GAO, and all systems under our administrative control.

GAO cites that a plan of actions and milestones (POA&M) for systems was not updated by EPA since 2011. EPA believes POA&M updates were provided to GAO. EPA will work with GAO to clarify this comment and respond to that consideration before the final report is issued.

Thank you for the opportunity to review and comment on GAO's draft report.

Sincerely,

A handwritten signature in black ink, appearing to read "J. Woolford".

James Woolford  
Acting Principal Deputy Assistant Administrator  
and Acting Deputy Chief Information Officer

# Appendix V: Comments from the Office of Personnel Management



Chief Information  
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT  
Washington, DC 20415

JUL 10 2014

Mr. Gregory C. Wilshusen  
Director  
Information Security Issues  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, DC 20548

Dear Mr. Wilshusen:

The Office of Personnel Management (OPM) recognizes that even the most well run programs can benefit from an external evaluation and we appreciate the input of the Government Accountability Office as we continue to enhance our contractor oversight program. We have reviewed your draft audit report (GAO-14-612) titled "Information Security: Agencies Need to Improve Oversight of Contractor Controls." A specific response to your recommendation is provided below.

Response to Recommendation

Recommendation: We recommend that the Director of the Office of Personnel Management develop, document and implement oversight procedures for ensuring that a system test is fully executed for each contractor-operator system.

Management Response: Concur. The OPM IT Security and Privacy Handbook provides policy for oversight of contractor systems, and the IT security office has published procedures to facilitate contractor systems oversight. We will review these existing security policies and procedures to further enhance OPM's oversight of contractor operated systems.

Sincerely,

  
Donna K. Seymour  
Chief Information Officer



# Appendix VI: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

July 8, 2014

Gregory C. Wilshusen  
Director, Information Security Issues  
U.S. Government Accountability Office  
441 G Street NW  
Washington, DC 20548

Re: Draft Report GAO-14-612, "INFORMATION SECURITY: Agencies Need to Improve Oversight of Contractor Controls"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that DHS is "taking actions to assist agencies in planning to improve their cybersecurity posture." The report did not contain any recommendations specifically directed at DHS. However, it contained one recommendation for the Director of the Office of Management and Budget (OMB) to, in collaboration with the Secretary of Homeland Security, develop and clarify reporting guidance to agencies for annually reporting the number of contractor-operated systems.

DHS, through its National Protection and Programs Directorate (NPPD), is committed to effectively carrying out its cyber security responsibilities and activities, including contractor oversight. For example, NPPD currently provides quarterly and annual metric reporting guidance to federal agencies on Federal Information Security Management Act (FISMA) compliance (<http://www.dhs.gov/publication/fy14-fisma-documents>). NPPD will collaborate with OMB and update this guidance, which includes language in reporting the number of contractor-operated systems, for the fiscal year 2015 FISMA reporting period, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim H. Crumpacker".

Jim H. Crumpacker, CIA, CFE  
Director  
Departmental GAO-OIG Liaison Office

---

# Appendix VII: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Gregory C. Wilshusen (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)

---

## Staff Acknowledgments

In addition to the individual named above, the following staff also made key contributions to the report: Nicholas Marinos (assistant director), Melina Asencio, Sher'rie Bacon, Kathleen Feild, Nancy Glover, Wilfred Holloway, Thomas Johnson, David Plocher, and Jeffrey Woodward.

---

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

---

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@gao.gov), (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

---

## Public Affairs

Chuck Young, Managing Director, [youngc1@gao.gov](mailto:youngc1@gao.gov), (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

