United States Government Accountability Office

Report to Congressional Requesters

June 2014

INFORMATION SECURITY

Additional Oversight Needed to Improve Programs at Small Agencies

GAO-14-344

GAO Highlights

Highlights of GAO-14-344, a report to congressional requesters

June 2014

INFORMATION SECURITY

Additional Oversight Needed to Improve Programs at Small Agencies

Why GAO Did This Study

Small federal agencies—generally those with 6,000 or fewer employees—are, like larger agencies, at risk from threats to information systems that support their operations and the information they contain, which can include personally identifiably information. Federal law and policy require small agencies to meet information security and privacy requirements and assign responsibilities to OMB for overseeing agencies' activities. OMB has assigned several of these duties to DHS.

GAO was asked to review cybersecurity and privacy at small agencies. The objectives of this review were to determine the extent to which (1) small agencies are implementing federal information security and privacy laws and policies and (2) OMB and DHS are overseeing and assisting small agencies in implementing their information security and privacy programs. GAO selected six small agencies with varying characteristics for review; reviewed agency documents and selected systems; and interviewed agency, OMB, and DHS officials.

What GAO Recommends

GAO recommends that OMB report on all small agencies' implementation of security and privacy requirements. GAO also recommends that DHS develop services and guidance targeted to small agencies' environments. GAO is making recommendations to the six agencies reviewed to address their information security and privacy weaknesses in a separate, restricted report. OMB and DHS generally concurred with the recommendations.

View GAO-14-344. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The six small agencies GAO reviewed have made mixed progress in implementing elements of information security and privacy programs as required by the Federal Information Security Management Act of 2002, the Privacy Act of 1974, the E-Government Act of 2002, and Office of Management and Budget (OMB) guidance (see figure).

Agencies' Implementation of Information Security and Privacy Elements in Fiscal Year 2013

Information Security

	Agency 1	Agency 2	Agency 3	Agency 4	Agency 5	Agency 6
Risk assessments	◐	◐	○	◐	○	◐
Policies & procedures	◐	◐	○	◐	○	◐
System security plans	◐	◐	○	◐	○	◐
Security training program	◐	◐	○	●	○	◐
Continuous monitoring of security controls	◐	◐	○	◐	○	◐
Remediation program	◐	◐	○	◐	○	◐
Incident response & reporting	◐	◐	○	◐	○	◐
Continuity of operations program	◐	◐	○	◐	○	◐

Privacy

	Agency 1	Agency 2	Agency 3	Agency 4	Agency 5	Agency 6
Issue system of records notices	●	◐	○	○	○	◐
Assign senior agency official for privacy	●	●	●	●	○	●
Conduct privacy impact assessments [a]	●	●	○	○	N/A	○

● Fully implemented ◐ Partially implemented ○ Did not implement

Source: GAO analysis of agency documentation. | GAO-14-344

[a] Agency 5 was not required to complete a privacy impact assessment.

In a separate report for limited official use only, GAO is providing specific details on the weaknesses in the six selected agencies' implementation of information security and privacy requirements.

OMB and the Department of Homeland Security (DHS) took steps to oversee and assist small agencies in implementing security and privacy requirements. For example, OMB and DHS instructed small agencies to report annually on a variety of metrics that are used to gauge implementation of information security programs and privacy requirements. In addition, OMB and DHS issued reporting guidance and provided assistance to all federal agencies on implementing security and privacy programs. However, 55 of 129 small agencies identified by OMB and DHS are not reporting on information security and privacy requirements. Further, the agencies in GAO's review have faced challenges in using the guidance and services offered. Until OMB and DHS oversee agencies' implementation of information security and privacy program requirements and provide additional assistance, small agencies will continue to face challenges in protecting their information and information systems.

United States Government Accountability Office

Contents

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
POA&M	plan of action and milestones
SP	Special Publication
TIC	Trusted Internet Connections
TSP	Thrift Savings Plan
US-CERT	United States Computer Emergency Readiness Team

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 25, 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 Susan M. Collins
United States Senate

Small agencies—those with 6,000 or fewer employees—like large agencies, place a great deal of sensitive information on their systems and, if not properly protected, they are at risk from the growing and evolving threats to the systems and networks that support federal operations.[1] These growing and evolving threats can potentially affect all segments of our society, including individuals, private businesses, government agencies, and other entities. Laws such as the Privacy Act of 1974,[2] the E-Government Act of 2002,[3] and the Federal Information Security Management Act (FISMA) of 2002[4] are meant to assist agencies by creating a framework for protecting information and information systems. 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, a designation that remains in place today.[5]

You asked us to review cybersecurity and privacy at small agencies. Our objectives were to determine the extent to which (1) small agencies are

[1] For this report, the term "small agencies" includes both small and micro agencies unless otherwise noted. According to the Office of Management and Budget, a small agency has fewer than 6,000 employees, and most have fewer than 500 staff. A micro agency has fewer than 100 employees.

[2] Pub. L. No. 93-579 (Dec. 31, 1974); 5 U.S.C. 552a.

[3] Pub. L. No. 107-347 (Dec. 17, 2002).

[4] Pub. L. No. 107-347, Title III (Dec. 17, 2002); 44 U.S.C. 3541.

[5] GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: February 2013).

implementing federal information security and privacy laws and policies and (2) the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) are overseeing and assisting small agencies with implementing their information security and privacy programs.

We selected the Federal Retirement Thrift Investment Board because of a significant data breach it experienced in 2012. Then, we selected the following five additional agencies to be included in our review: the Federal Trade Commission; the International Boundary Commission, United States and Canada; the James Madison Memorial Fellowship Foundation; the National Capital Planning Commission; and the National Endowment for the Humanities. To select these five agencies, we compiled a listing of small agencies, and categorized the agencies into five primary areas, selecting one agency from each area. Because of the small number of agencies reviewed, our findings are not representative of any population of small agencies and our results only apply to the six selected agencies.

We reviewed and analyzed documents from the selected agencies, including information security and privacy policies, plans, and procedures; reviewed the testing of controls and performed tests of selected controls over selected key systems; interviewed agency officials; and reviewed inspector general reports to determine whether selected agencies were implementing information security and privacy requirements. We also interviewed OMB and DHS officials regarding their actions in overseeing and assisting agencies in meeting information security and privacy requirements. In addition, we interviewed officials from the selected agencies regarding their interactions with OMB and DHS.

We conducted this performance audit from January 2013 to June 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. See appendix I for additional details on our objectives, scope, and methodology.

Background

Safeguarding government computer systems and sensitive information, including personally identifiable information (PII)[6] that resides on them, is an ongoing challenge due to the complexity and interconnectivity of systems, the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. To help address this challenge, federal agencies, regardless of their size, must abide by federally mandated standards, guidelines, and requirements related to federal information systems.

Federal Law Established Information Security Program Requirements

FISMA established a framework designed to ensure the effectiveness of security controls for information and information systems that support federal operations and assets. FISMA assigns specific responsibilities to (1) OMB, to develop and oversee the implementation of policies, principles, standards, and guidelines on information security (except with regard to national security systems); to report, at least annually, on agency compliance with the act; and to approve or disapprove agency information security programs; (2) agency heads, to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; (3) agency heads and chief information officers, to develop, document, and implement an agency-wide information security program; (4) inspectors general, to conduct annual independent evaluations of agency efforts to effectively implement information security; and (5) the National Institute of Standards and Technology (NIST), to develop standards and guidance to agencies on information security.

More specifically, FISMA requires each agency to develop, document, and provide 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;

[6] PII 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.

- policies and procedures that (1) are 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;
- 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 of information security risks and of their responsibilities in implementing agency policies and procedures, 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 major 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.

FISMA also gives OMB responsibility for ensuring the operation of a federal information security incident center. Established in 2003, the United States Computer Emergency Readiness Team (US-CERT) is the federal information security incident center mandated by FISMA. US-CERT consults with agencies on cyber incidents, provides technical information about threats and incidents, compiles the information, and publishes it on its website, https://www.us-cert.gov.

In the 11 years since FISMA was enacted, executive branch oversight of agency information security has changed. As part of its FISMA oversight responsibilities, OMB has issued annual guidance to agencies on implementing FISMA requirements, including instructions for agency and inspector general reporting. However, in July 2010, the Director of OMB and the White House Cybersecurity Coordinator issued a joint memorandum stating 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.[7] The memorandum stated that DHS's activities would include

- overseeing the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance;
- overseeing and assisting government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity;
- overseeing the agencies' compliance with FISMA and developing analyses for OMB to assist in the development of the FISMA annual report;
- overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance; and
- annually reviewing the agencies' cybersecurity programs.

Within DHS, the Federal Network Resilience Office, within the National Protection and Programs Directorate, is responsible for (1) developing and disseminating most FISMA reporting metrics, (2) managing the CyberScope[8] web-based application, and (3) collecting and reviewing federal agencies' cybersecurity data submissions and monthly data feeds to CyberScope. In addition, the office is responsible for conducting cybersecurity reviews and assessments at federal agencies to evaluate the effectiveness of agencies' information security programs.

Requirements for Privacy Protections Created in Law and Guidance

The primary laws that require privacy protections for personal information maintained, collected, used, or disseminated by federal agencies are the Privacy Act of 1974 and the E-Government Act of 2002. The Privacy Act places limitations on agencies' collection, maintenance, disclosure, and use of PII maintained in systems of records, including requirements for each agency to (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required by statute or by executive order of the President; (2) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in

[7] 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).

[8] CyberScope is an interactive data collection tool that has the capability to receive data feeds on a recurring basis to assess the security posture of a federal agency's information infrastructure. Agencies are required to use this tool to respond to reporting metrics.

maintaining any record, and instruct each such person in those rules and the requirements of the act; and (3) establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[9] Additionally, when an agency establishes or makes changes to a system of records, it must notify the public through a system of records notice in the *Federal Register* that includes the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personally identifiable information.

In addition, the E-Government Act of 2002 requires agencies to assess the impact of federal information systems on individuals' privacy. Specifically, the E-Government Act strives to enhance the protection of personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA) for systems or collections containing personal information. According to OMB guidance, the purpose of a PIA is to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Small Agencies Provide a Variety of Government Services

Small agencies provide a variety of services and manage a variety of federal programs. According to OMB, their responsibilities include issues concerning commerce, trade, energy, science, transportation, national security, finance, and culture. Approximately half of the small agencies in the federal government perform regulatory or enforcement roles in the executive branch. For example, the National Archives and Records Administration oversees the federal government's recordkeeping and

[9] The Privacy Act defines a "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier.

ensures preservation of and access to records. In addition, the Federal Reserve Board assists with implementing the monetary policy of the United States. The Federal Reserve Board also plays a major role in the supervision and regulation of the U.S. banking system.

The remaining small federal agencies are largely grant-making, advisory, and uniquely chartered organizations. For example, the United States Institute of Peace is an independent, nonpartisan institution established and funded by Congress to increase the nation's capacity to manage international conflict without violence. Together, small agencies employ about 90,000 federal workers and manage billions of taxpayer dollars.

Similarly, the six selected agencies in our review provide a broad range of federal services (see table 1).

Table 1: Selected Small Agencies Included in GAO's Review

Agency	Description	Classification
Federal Retirement Thrift Investment Board	Administers the Thrift Savings Plan (TSP), a tax-deferred, defined-contribution plan, similar to private sector 401(k) plans, which provides federal employees and members of the uniformed services the opportunity to save for additional retirement security. The TSP is part of the Federal Employment Retirement System.	Micro
Federal Trade Commission	Prevents business practices that are anticompetitive, deceptive, or unfair to consumers, to enhance informed consumer choice and public understanding of the competitive process, and to accomplish this without unduly burdening legitimate business activity.	Small
International Boundary Commission, United States and Canada	Determines the position of any point on the U.S. and Canadian boundary necessary to settle questions that might arise between the United States and the Canadian government.	Micro
James Madison Memorial Fellowship Foundation	Provides graduate fellowships to individuals desiring to become outstanding teachers of the American Constitution at the secondary school level.	Micro
National Capital Planning Commission	Protects and enhances historical, cultural, and natural resources of the National Capital Region by crafting long-range plans, analyzing emergent planning issues, reviewing site development and building proposals, and monitoring federal capital investment.	Micro
National Endowment for the Humanities	Advances the knowledge and understanding in the humanities in the United States and provides national leadership in promoting the humanities in American life through grants.	Small

Source: GAO based on agency data. | GAO-14-344

Information Security Incidents at Small Agencies

Small federal agencies have reported a number of incidents that have placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. According to DHS, the number of reported security incidents for small agencies from fiscal year 2009 to fiscal year 2013 ranged from 2,168 to 3,144. Incidents involving PII at small agencies increased from 258 in fiscal year 2009 to 664 in fiscal year 2013. In addition, in fiscal year 2013, small agencies reported 2,653 incidents to US-CERT. Table 2 describes the incident categories as defined by US-CERT.

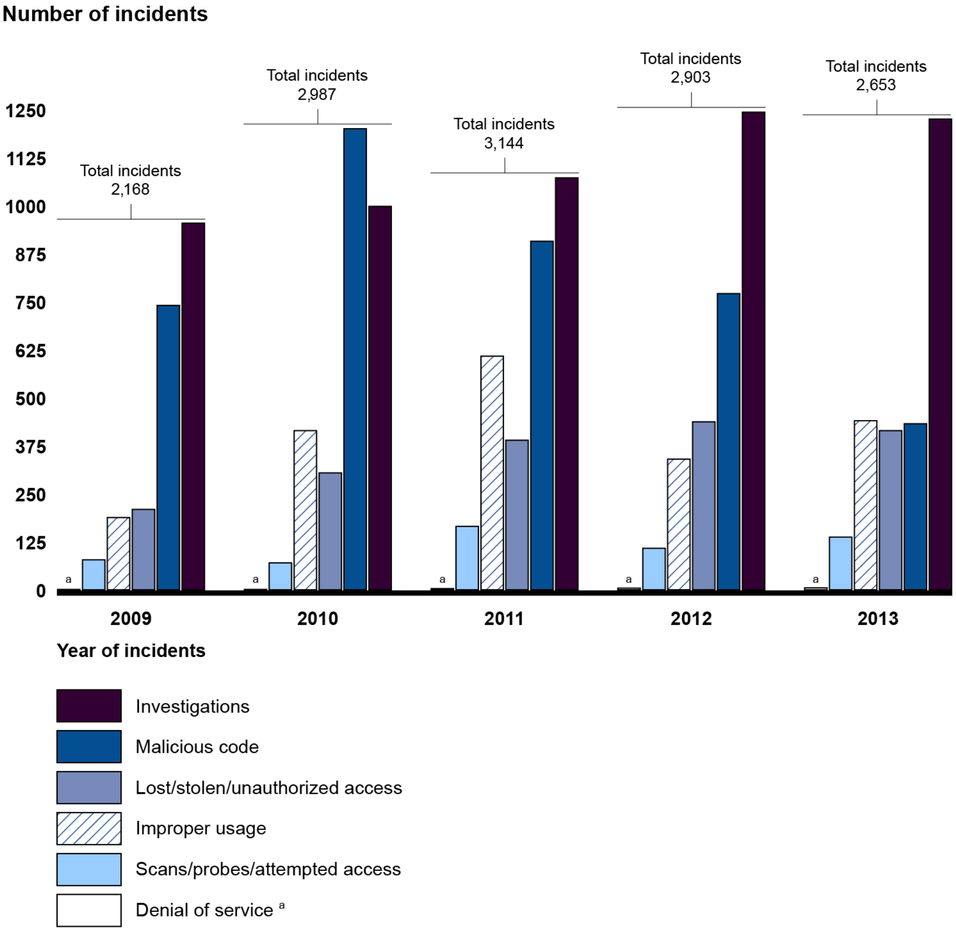
Table 2: United States Computer Emergency Readiness Team Information Security Incident Definitions

Category	Incident definition
Unauthorized Access	All incidents where an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
Denial of Service	All successful attacks that prevent or impair the normal authorized functionality of networks, systems, or applications by exhausting resources.
Malicious Code	All successful installations of malicious software that infect an operating system or application.
Improper Usage	All incidents where a user violates acceptable computing use policies.
Scans/Probes/Attempted Access	Any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit.
Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Source: GAO based on DHS-supplied data. | GAO-14-344

As shown in figure 1, the three most prevalent types of incidents reported by small agencies to US-CERT during fiscal year 2013 were those involving potentially malicious or anomalous activity (investigation), the execution or installation of malicious software (malicious code), and the violation of acceptable computing use policies (improper usage).

Figure 1: Information Security Incidents at Small Agencies, Fiscal Years 2009 – 2013



Source: GAO based on US-CERT-supplied data. | GAO-14-344

[a] In fiscal year 2009 and 2010, one denial of service was reported in each year; in fiscal year 2011, three were reported; in fiscal year 2012, four were reported; and in fiscal year 2013, five were reported.

Selected Small Agencies Have Made Mixed Progress in Implementing Federal Information Security and Privacy Requirements

Although the small agencies we reviewed have taken steps to develop information security and privacy programs, weaknesses existed that threatened the confidentiality, integrity, and availability of their information and systems. Regarding information security, these agencies did not fully or effectively develop, document, and implement security plans, policies, and procedures, as well as other elements of an information security program such as incident handling and contingency planning. A key reason for these weaknesses is that these small agencies have not yet fully implemented their agency-wide information security programs to ensure that controls are appropriately designed and operating effectively, and two of the six agencies did not develop an information security program that included any of the required FISMA elements. In addition, five of the six selected agencies had not fully implemented their privacy programs to ensure protection of PII. For example, while most of the six agencies designated a privacy official, not all the agencies completed privacy impact assessments. Further, two of the six agencies we reviewed had not implemented any of the selected privacy requirements. As a result, these selected agencies have limited assurance that their PII and information systems are being adequately protected against unauthorized access, use, disclosure, modification, disruption, or loss.

Most Small Agencies Reviewed Have Developed Elements of an Information Security Program, but Implementation Has Been Mixed

The six small agencies we reviewed have generally developed many of the requirements of an information security program, but these programs have not been fully implemented. Specifically, four of the six agencies have developed an information security program that includes risk assessments, security policies and procedures, system security plans, security awareness training, periodic testing and evaluation, remedial action plans, incident handling, and contingency planning. However, key elements of their plans, policies, or procedures in these areas were outdated, incomplete, or did not exist. In addition, two of the six agencies did not develop an information security program with the required FISMA elements.

Most of the Six Selected Agencies Had Outdated or Missing Risk Assessments

FISMA requires each agency to develop, document, and implement an information security program that includes 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. According to NIST's *Guide for Conducting Risk Assessments*, risk is determined by identifying potential threats to the organization, identifying vulnerabilities in the organization's systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data.[10] NIST guidance states that risk assessments should include essential elements such as discussion of threats, vulnerabilities, impact, risk model, and likelihood of occurrence, and be updated based on a frequency defined by the organization.

Four of the six selected agencies developed and conducted risk assessments. For example, one agency's risk assessment generally adhered to NIST guidance for conducting risk assessments. Specifically, it included information related to the identification of threats, vulnerabilities, and impacts, and recommended corrective actions for mitigating or eliminating the threats and vulnerabilities that were identified. However, the risk assessment did not identify the assumptions and constraints associated with the assessment. Another agency developed a risk management framework and documented a risk assessment policy but had not completed risk assessments for its systems. In addition, risk assessments at the four agencies were outdated or did not include elements outlined in NIST guidance, as the following examples illustrate.

- At one selected agency, risk assessments for the four systems reviewed were not updated based on the agency's policy of updating its risk assessments annually. Specifically, risk assessments for three of the four systems had not been conducted since 2005, 2009, and 2010, respectively. While the remaining system had an assessment conducted in 2013, the prior assessment for that system was done in 2010. Additionally, risk assessments for three of the four systems lacked essential elements such as a list of vulnerabilities unique to the individual systems, and one of the assessments did not assess the likelihood of an incident occurring or determine the risk level. The fourth assessment, which was dated 2005, was updated during our review but did not address threats, vulnerabilities, and likelihood of incident occurrence or risks. Agency officials stated that while the risk assessments were outdated, they have conducted informal and formal risk assessments that were not documented. The agency plans to formalize and document its risk assessments to align with its own policies and NIST standards by June 2014.

[10] NIST, *Guide for Conducting Risk Assessments*, Special Publication (SP) 800-30 (Gaithersburg, Md.: September 2012).

- Another agency in our review did not identify in its risk assessments the system threats and vulnerabilities, and did not recommend corrective actions for mitigating the threats and vulnerabilities for the three systems we reviewed. According to agency officials, new risk assessments will be conducted for all three of the systems we reviewed in 2014.
- The remaining two agencies, which did not conduct risk assessments for their systems, cited various reasons for not completing them. One agency stated it was not aware of the requirement to conduct risk assessments. The other agency stated that it received a waiver from OMB for complying with FISMA requirements. According to OMB officials, they have not granted FISMA waivers to any federal agency and FISMA does not allow for waivers.

Without current, complete risk assessments, agencies are at an increased probability of not identifying all threats to operations and may not be able to mitigate risks to a level appropriate to meet minimum requirements.

The Six Selected Small Agencies Had Outdated, Incomplete, or Missing Policies and Procedures

A key element of an effective information security program, as required by FISMA, is to develop, document, and implement risk-based policies and procedures that govern the security over an agency's computing environment. According to NIST, an organization should develop, document, and disseminate (1) a policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and (2) procedures to facilitate the implementation of the policy and associated controls. Procedures are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task. If properly implemented, policies and procedures may be able to effectively reduce risk to the information and information systems.

Four of the six small agencies we reviewed had documented information security policies and procedures, and two did not. For example, in fiscal year 2012, one of the selected agencies documented policies that addressed each of the FISMA elements as a part of its information security program. Another agency had policies addressing risk assessments, security plans, security awareness and training, periodic testing and evaluation, remedial actions, incident response, and contingency planning. However many, but not all, of the policies and procedures documented by the six agencies were either outdated, incomplete, or did not exist (see fig. 2).

Figure 2: Six Selected Agencies' Documentation of Policies and Procedures for Information Security Program Elements

		Agency 1	Agency 2	Agency 3	Agency 4	Agency 5	Agency 6
Risk management	Policies	◐	⊘	●	⊘	●	●
	Procedures	⊘	⊘	⊘	⊘	⊘	⊘
Security planning	Policies	⊘	⊘	●	⊘	●	●
	Procedures	⊘	⊘	⊘	⊘	●	⊘
Security awareness training	Policies	◐	⊘	●	⊘	◐	●
	Procedures	◐	⊘	◐	⊘	●	⊘
Remediation	Policies	⊘	⊘	●	⊘	◐	●
	Procedures	⊘	⊘	◐	⊘	⊘	◐
Perodic testing and evaluation	Policies	◐	⊘	●	⊘	●	●
	Procedures	⊘	⊘	◐	⊘	⊘	⊘
Incident response and reporting	Policies	◐	⊘	●	⊘	◐	●
	Procedures	◐	⊘	⊘	⊘	◐	●
Contingency planning	Policies	◐	⊘	●	⊘	◐	●
	Procedures	◐	⊘	⊘	⊘	◐	⊘

● Current and complete ◐ Outdated or incomplete ⊘ Did not exist

Source: GAO analysis of agency documentation. | GAO-14-344

- For instance, agency 1 had information security policies that had not been updated since 2001. During our review, the agency hired a contractor to develop a new information technology (IT) security framework based on NIST guidance,[11] with a planned completion date of the end of 2014. According to an agency official, a new entity-wide information security policy was documented and implemented in December 2013. We reviewed a copy of the policy and determined it addressed each of the eight elements of an information security program mandated by FISMA.
- Agencies 2 and 4 had not developed, documented, or implemented any information security policies or procedures. They stated that it did not have a true understanding of information security program requirements. According to officials at one of these agencies, they

[11] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Special Publication (SP) 800-37, Revision 1 (Gaithersburg, Md.: February 2010).

had not developed policies or procedures because they were not aware of these requirements and lacked the technical staff to address this area.

- Agency 3 documented a policy for incident handling but lacked procedures. According to an official at this agency, the agency uses a NIST checklist as its documented procedures. However, according to NIST, the actual steps performed may vary based on the type of incident and the nature of individual incidents.
- Agency 5 documented implementation procedures for incident response, but did not document risk assessment procedures.
- Agency 6 established policies for the seven information security program elements. The agency documented procedures for incident handling and established draft documented procedures for remediation but lacked documented procedures for the remaining elements. According to agency officials, the remaining procedures will be documented by June 2014.

Until the selected agencies fully develop and update their policies and procedures to govern the security over their computing environments, they will have limited assurance that controls over their information are appropriately applied to their systems and operating effectively.

Most of the Six Selected Agencies Lacked Current or Complete System Security Plans

FISMA requires an agency's information security program to include plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. According to NIST, the purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.[12] The first step in the system security planning process is to categorize the system based on the impact to agency operations, assets, and personnel should the confidentiality, integrity, and availability of the agency information and information systems be compromised. This categorization is then used to determine the appropriate security controls needed for each system.

Four of the six selected agencies developed system security plans. For example, one agency completed system security plans that identified the categorization level and appropriate security controls, based on NIST

[12] NIST, *Guide for Developing Security Plans for Information Technology Systems*, Special Publication (SP) 800-18 (Gaithersburg, Md.: February 2006).

800-53,[13] for each of the four systems reviewed. Another agency also completed security plans and categorizations for the one system we reviewed.

However, system security plans for these four agencies were missing elements or outdated.

- At one agency, while three of the four system security plans we reviewed included items such as system owners and authorizing officials, these plans did not include completion and approval dates. The fourth plan included a completion date but did not have an approval date, and two of the four plans were outdated. One plan had not been updated since 2009, and the other had not been updated since 2011. The agency did not have a standardized template for creating security plans, which led to the inconsistencies in the various plans. The agency plans to standardize its security plans and update plans for three of the four systems selected for review by June 2014. The fourth system will be replaced and retired by June 2014.
- Another agency developed system security plans for three of its systems. However, two of the three were outdated. One plan has not been updated since 2009, and the other has not been updated since 2011. According to agency officials, the agency plans to update all three system security plans in 2014.
- A third agency divided its general support system into 21 systems and major applications. In fiscal year 2013, it completed security plans and categorizations for 1 of its systems. According to an agency official, the security plan for another system was completed in fiscal year 2014 and the security plans for the remaining 19 systems and major applications are scheduled to be completed by March 2015.
- A fourth agency developed and documented a system security plan but referenced policies and procedures from February 2001. According to an agency official, the security plan will be updated to address the appropriate security controls and reflect the agency's new IT security policy.

Finally, the remaining two agencies had not considered the need for system security plans for their systems. Agency officials at both agencies stated they were unaware of this requirement; as a result, they did not take steps to determine if a system security plan was needed for their

[13] NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 3 (Gaithersburg, Md.: August 2009).

systems. Until these selected agencies appropriately develop and update system security plans, they may face an increased risk that officials will be unaware of system security requirements and that controls are not in place.

Most of the Six Selected Small Agencies Generally Completed Security Awareness Training Programs but Did Not Complete Specialized Training

FISMA requires agencies to provide security awareness training to personnel, including contractors and other users of information systems that support the operations and assets of the agency. Training is intended to inform agency personnel of the information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. FISMA also requires agencies to provide specialized training to personnel with significant security responsibilities. Providing training to agency personnel is critical to securing information and information systems since people are one of the weakest links in attempts to secure systems and networks.

Four of the six selected agencies developed a security awareness training program, and one of these four agencies completed specialized training for employees with significant security responsibilities.

- One of the four agencies implemented a new web-based security awareness training program in 2013. This agency trained 100 percent of its employees. However, the agency did not have specialized security training for the individuals with significant security responsibilities. According to agency officials, the agency obtained funds and purchased specialized training and plans to complete this training in 2014.
- Another agency updated its security awareness program in fiscal year 2013, and 100 percent of its users completed annual security awareness training. The agency developed specialized training, but not all required individuals with significant security responsibilities had taken it. According to officials, the agency's tracking of specialized training is not automated and it has been difficult to get all required employees together to take the training. Specialized training was identified as an issue in the agency's fiscal year 2012 inspector general report, and the agency is working to establish goals for a more comprehensive tracking system for its specialized training.
- A third agency developed a security awareness program and trained 95 percent of its users. According to agency officials, users who did not complete the training were either interns that completed the initial training, external auditors, executives, or remote users. In addition, we found that four out of nine users requiring specialized training did not take it in fiscal year 2013. According to an agency official, insufficient

funding was the reason that the users did not take the required training. The agency plans for the users to take specialized training in fiscal year 2014.

- The fourth agency trained 100 percent of its users during fiscal year 2013. We found that users requiring specialized security training received it during fiscal year 2013.
- The remaining two selected agencies had neither conducted annual security awareness training for all of their employees nor provided specialized training for security personnel. Officials at one of the agencies stated that two of its employees received security awareness training through another federal agency, but its remaining employees had not received such training. Officials at the other agency stated that the agency does not conduct any formal security awareness training due to its small size.

Without fully developing and implementing a security awareness program, including training for users with significant security roles, the selected agencies may not have the proper assurance that their personnel have a basic awareness of information security issues and agency security policies and procedures. In addition, agencies that did not provide specialized training may not have reasonable assurance that staff with significant system security roles have the adequate knowledge, skills, and abilities consistent with their roles to protect the confidentiality, integrity, and availability of the information housed within the information systems to which they are assigned.

The Six Selected Agencies Did Not Effectively Test and Evaluate the Effectiveness of Information Security Policies, Procedures, and Practices

FISMA requires that federal agencies periodically test and evaluate the effectiveness of their information security policies, procedures, and practices as part of implementing an agency-wide security program. This testing is to be performed with a frequency depending on risk, but no less than annually. Testing should include management, operational, and technical controls for every system identified in the agency's required inventory of major systems.

Four of the six selected agencies conducted periodic testing and evaluation of their systems. However, their tests were incomplete and not conducted at least annually, as required. The following examples illustrate these weaknesses:

- One agency documented that security assessments were conducted for the three systems reviewed, but the assessments did not clearly identify which management, operational, and technical controls were tested or reviewed. Additionally, the controls for the three systems had not been tested or reviewed at least annually. Specifically, one system was last tested in December 2008 and the other two systems were last tested in September 2009 and October 2010, respectively. According to an agency official, the security assessments will be updated in 2014.

- At another agency, security tests and evaluations were conducted as a part of the system assessment and authorization process. According to agency officials, the agency completed the security test and evaluations for 2 of its 21 systems and major applications in 2013. It plans to complete the remaining 19 assessment and authorizations by March 2015.
- A third agency hired an independent contractor in fiscal year 2012 to test or review management, operational, and technical controls for its general support system. However, the contractor did not test all controls for the system. According to an agency official, controls not tested were not within the contracted scope of the assessment. The agency plans to conduct a security assessment and authorization for its new system in fiscal year 2014.
- The fourth agency lacked sufficient documentation to show that assessments were performed annually. For example, one of the systems selected for review was last tested in 2010 or 2011. The assessments for the other two systems did not identify when the testing of controls occurred, and the agency could not provide documentation to show when it occurred.

Further, two of the six selected agencies did not have periodic testing and evaluation programs and did not test the security controls of their systems. According to those agency officials, it was not clear that this was an area that needed to be addressed.

Without appropriate test and evaluation, agencies may not have reasonable assurance that controls over their systems are being effectively implemented and maintained.

The Six Small Agencies Reviewed Did Not Fully Document Remedial Action Plans

FISMA requires agencies to plan, implement, evaluate, and document remedial actions to address any deficiencies in their information security policies, procedures, and practices. In its fiscal year 2012[14] and 2013[15] FISMA reporting instructions, OMB emphasized that remedial action plans—known as plans of action and milestones (POA&M)—are to be the authoritative agency-wide management tool for addressing information security weaknesses. In addition, NIST guidance states[16] that federal agencies should develop a POA&M for information systems to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system. NIST guidance also states that organizations should update existing POA&Ms based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. According to OMB, remediation plans assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Four of the six selected agencies documented remedial action plans to address identified weaknesses. For instance, one of the agencies documented remedial action plans and included weaknesses identified from security assessments in the POA&M for one of its systems. At another agency, remedial actions to correct weaknesses noted during its assessment were documented.

While these four agencies documented remedial action plans, plans were missing elements as required by OMB. For example, one agency's POA&Ms lacked either estimated completion dates or the actual completion date of corrective actions that remediated identified weaknesses. Another agency's POA&Ms lacked elements such as estimated funding sources, severity ratings, milestone completion dates, or changes to milestone completion dates where applicable.

[14] Fiscal year 2012 reporting instructions were issued by OMB as M-12-20 (Sept. 27, 2012).

[15] Fiscal year 2013 reporting instructions were issued by OMB as M-14-04 (Nov. 18, 2013).

[16] NIST 800-53, Revision 3.

Further, two of the six selected agencies did not develop or document remedial action plans. According to agency officials, neither agency was aware of the requirements to document remedial actions.

Without an effective process for planning, implementing, evaluating, and documenting remedial actions, these agencies cannot ensure they are addressing deficiencies in their information security policies, procedures, and practices.

The Six Selected Agencies Did Not Fully Document or Test Plans or Procedures for Detecting, Reporting, and Responding to Security Incidents

FISMA requires that agency security programs include procedures for detecting, reporting, and responding to security incidents, including reporting incidents to US-CERT.[17] According to NIST, agencies should create an incident response policy and use it as the basis for incident response procedures.[18] The procedures should then be tested to validate their accuracy and usefulness. The ability to identify incidents using appropriate audit and monitoring techniques enables an agency to initiate its incident response plan in a timely manner. Once an incident has been identified, an agency's incident response procedures should provide the capability to correctly log the incident, properly analyze it, and take appropriate action.

Four of the six small agencies we reviewed had taken steps to develop policies and procedures as required by FISMA and recommended by NIST guidance for incident handling.[19] Specifically, these agencies' policies and procedures included incident response policies or plans, incident response team policy, procedures for US-CERT notification, and escalation procedures for information security incidents. One agency, for example, had documented policy and procedures for detecting, reporting, and responding to security incidents that required personnel to report incidents involving personally identifiable information to the Chief Information Officer within 1 hour, and all other types of incidents to the agency's Security Officer.

[17] According to NIST, a security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur.

[18] NIST, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61, Revision 2 (Gaithersburg, Md.: August 2012).

[19] NIST, Special Publication 800-61.

However, these four agencies had not fully documented or tested their incident response policies and procedures. For example:

- One agency had not updated its incident response policy and plan since 2001. During the course of our review, in December 2013, the agency updated its incident response policy. According to agency officials, incident management is currently an ad hoc process. Incident management will be included in agency-wide procedures due to be completed in 2014. Between fiscal year 2011 and 2013, the agency reported one incident to US-CERT.
- Another agency has developed and documented an incident response policy but has not documented procedures for responding to security incidents. According to agency officials, the agency is in the process of developing and documenting an incident response plan with procedures. The agency has taken these actions to improve its incident detection and reporting capabilities and awarded a contract to acquire services to both improve and support these capabilities. According to agency officials, this agency reported one incident from fiscal year 2011 to fiscal year 2013.
- The third agency had documented policies and procedures for its incident response program but had not followed its own policy for testing the incident response plan. According to an agency official, members of the team were aware of the plan and its procedures. Between fiscal year 2011 and fiscal year 2013, this agency reported six incidents to US-CERT.
- The fourth agency had documented policies and procedures for its incident response program but had not followed its policy for testing its incident response practices. While the agency did not perform testing in 2012, it did test its incident response capability in 2013. According to agency officials, the agency reported eight incidents in fiscal year 2012 and fiscal year 2013.

Furthermore, two of the six selected agencies had not developed or documented policies or procedures for incident response. According to officials of one of the agencies, the only incidents it experienced are viruses, and its ad hoc process is to remove the virus from the laptop. If it cannot be removed, the agency replaces the laptop. At the second agency, officials stated that they had one known incident, which they believed was a phishing attack. According to an agency official, incidents would be reported or handled by their contractor. However, the contractor could not demonstrate that it had documented incidents or procedures for responding to incidents. According to officials for both agencies, no incidents were reported to US-CERT from fiscal year 2011 through fiscal year 2013. The agencies currently do not have plans to create documented incident response plans or procedures.

Without effective policies and procedures, these agencies may be hampered in their ability to detect incidents, report incidents to authorities such as US-CERT, minimize the resultant loss and destruction, mitigate the exploited weaknesses, and restore services.

Continuity of Operations Programs at the Six Selected Agencies Were Not Fully Implemented

FISMA requires federal agencies to develop and document plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. According to NIST,[20] contingency planning is part of overall information system continuity of operations planning, which fits into a much broader security and emergency management effort that includes, among other things, organizational and business process continuity and disaster recovery planning. These plans and procedures are essential steps in ensuring that agencies are adequately prepared to cope with the loss of operational capabilities due to a service disruption such as an act of nature, fire, accident, or sabotage. According to NIST, these plans should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, training personnel in their contingency roles and responsibilities and providing refresher training, and testing them and making necessary adjustments.

Four of the six selected agencies developed contingency planning documents. These four agencies took steps to implement FISMA requirements and NIST specifications, but have not fully met all requirements. For example:

- One agency had developed a draft contingency plan for the one system we reviewed but had not yet finalized or approved it. The agency also did not follow its own procedures and did not test the contingency plan. According to agency officials, emergency response training was provided to staff 2 years ago, and its staff meets every few months to ensure that all individuals are aware of their responsibilities in case of an emergency. The agency plans to finalize

[20] NIST, *Contingency Planning Guide for Federal Information Systems,* NIST Special Publication 800-34, Revision 1 (Gaithersburg, Md.: May 2010).

and test the plan but did not have a final date by when this would be done.

- Another agency completed and tested its disaster recovery plan[21] in fiscal year 2013. However, it has not provided contingency training to its employees or defined the frequency with which training should be conducted. The agency is scheduled to complete these items in December 2014.
- A third agency had documented a continuity of operations plan[22] that contained a disaster recovery plan. However, contingency plans were not developed or tested for its three information systems. Additionally, according to one agency official, the disaster recovery plan for the agency is outdated. According to the agency's inspector general FISMA report for fiscal year 2013, the agency did not test the plan in 2013 due to competing demands (e.g., a pending office move and launch of a new software program). According to agency officials, the agency intends to reinstitute the annual test exercises in fiscal year 2014. The inspector general's report noted that the agency implemented the core policies and procedures associated with contingency planning, including the creation of a business continuity plan, disaster recovery plan, continuity of operations plan exercises, signature of an alternate processing site agreement, and data backups. According to an agency official, the plans will be updated once the agency moves to its new location in fiscal year 2014.
- Additionally, the fourth agency's inspector general identified contingency planning as a weakness in fiscal year 2012. The inspector general reported that the agency did not have a final contingency plan or disaster recovery plan. In addition, the agency lacked a disaster recovery site and did not appropriately test its contingency plan. In fiscal year 2013, the inspector general reported that the agency (1) initiated a program to establish an enterprise-wide business continuity/disaster recovery program, (2) planned to have a disaster recovery site by the end of fiscal year 2014, and (3) tested its draft contingency plan and disaster recovery. In March 2014, the agency finalized its contingency plan and disaster recovery plan.

[21] According to NIST, a disaster recovery plan is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

[22] According to NIST, a continuity of operations plan is a predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Further, two of the six agencies have not developed contingency plans. According to an official at one of the agencies, the data used for their work are stored on the individual's laptop and each employee is required to back up their data. If the laptop or data are lost, the employee is responsible for restoring the data from the back-up. Otherwise, the employee would have to recreate the data. Without formal back-up procedures, the agency is at risk for lost data. Officials at the other agency stated that they did not have concerns about the potential loss of operations. If they were unable to operate, they would still be able to process payments and collect data since those operations are handled by another federal agency and contractor.

The uneven implementation of a comprehensive continuity of operations program by the six agencies could lead to less effective recovery efforts and may prevent a successful and timely system recovery when service disruptions occur. Additionally, without appropriate testing, these agencies cannot ensure they can adequately recover from a disaster.

In a separate report for limited official use only, we are providing specific details on the weaknesses in the six selected agencies' implementation of information security requirements.

The Six Selected Small Agencies Have Made Mixed Progress in Implementing Federal Privacy Requirements

The major statutory requirements for the protection of personal privacy by federal agencies are the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002. In addition, FISMA, which is included in the E-Government Act of 2002, addresses the protection of personal information in the context of securing federal agency information and information systems. Beyond these laws, OMB and NIST have issued guidance for assisting agencies with implementing federal privacy laws.[23] According to the Privacy Act, each agency that maintains a system of records shall, among other things, maintain in its records only such information about an individual as is relevant and necessary to accomplish a required purpose of the agency. Additionally, when an agency establishes or makes changes to a system of records, it must notify the public through a system of records notice in the *Federal*

[23] See, e.g., *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003); *Designation of Senior Agency Officials for Privacy*, M-05-08 (Feb. 11, 2005); and *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007).

Register. The notice should include items such as the categories of data collected, the categories of individuals about whom information is collected, the intended “routine” uses of data, and procedures that individuals can use to review and correct personally identifiable information.[24] According to OMB guidance, system of records notices should also be up to date.

The E-Government Act requires that agencies conduct privacy impact assessments (PIA) for systems or collections containing personal information. In addition, agencies must ensure the review of the PIA and, if practicable, make the PIA publicly available through the agency’s website, publication in the *Federal Register*, or other means. OMB guidance elaborates on the PIA process by stating, for example, that agencies are required to conduct PIAs when a system change creates new privacy risks (e.g., changing the way in which personal information is being used). According to OMB, the PIA requirement does not apply to all systems. For example, no assessment is required when the information collected relates to internal government operations, the information has been previously assessed under an evaluation similar to a PIA, or when privacy issues are unchanged.

The Privacy Act states that agencies must establish rules of conduct for persons involved in the design, development, operation, or maintenance of any systems of records, and establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. According to NIST,[25] privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. Accountability and commitment to the protection of individual privacy includes the appointment of a senior agency official for privacy, as required by OMB. The senior agency official should have overall responsibility for ensuring the agency’s implementation of information privacy protections, including the agency’s full compliance with federal

[24] Under the Privacy Act of 1974, the term “routine use” means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[25] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication (SP) 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

laws, regulations, and policies relating to information privacy, such as the Privacy Act.

The six small agencies we reviewed had made mixed progress in implementing these selected privacy requirements, as the following illustrates:

- *Issue system of records notices:* Most of the small agencies reviewed did not consistently issue notices. One agency appropriately issued system of records notices, two agencies posted notices that were no longer current, and three agencies did not issue any notices for systems requiring them. Of the two agencies with out-of-date system of records notices, one agency is determining which information systems contain information that will require system of records notices. Consequently, an official from this agency stated that the agency needed to update its 2005 notice. Similarly, an official from the other agency stated that the agency's system of records notices will be updated when the agency moves to a new location in fiscal year 2014. Among the three agencies that did not issue system of records notices, officials at two agencies did not believe that they were responsible for issuing the notices. While one of the agencies did not maintain PII in its system, the agency maintained paper files with PII that was covered by the Privacy Act and thus was responsible for issuing a system of records notice. An official from the second agency believed that other agencies were responsible for completing system of records notices on its behalf. An official from the third agency stated that the agency would revisit system of records notices as part of the reauthorization process for its systems.
- *Conduct privacy impact assessments*: Most of the selected small agencies did not consistently conduct privacy impact assessments for all systems containing personally identifiable information. Two agencies conducted privacy impact assessments for systems containing PII. Three agencies did not complete any assessments. The sixth agency was not required to perform an assessment because it did not maintain any systems containing personally identifiable information.

  Regarding the three agencies that did not complete PIAs, officials offered a variety of reasons for why they were not conducted. An official from one of the three agencies originally stated they did not maintain any information systems containing personal information related to employees or members of the public. However, we determined that this agency's general support system stored e-mail addresses for members of the general public, and therefore a privacy impact assessment should have been completed. An official from the second agency stated they will determine whether the systems containing PII would need a privacy impact assessment. The third agency did not conduct privacy impact assessments because officials inappropriately believed that a waiver from OMB relieved them from the requirement of preparing privacy impact assessments. However, no waivers exist for conducting privacy impact assessments, and OMB does not issue such waivers.

- *Assign senior official for privacy:* Most of the six selected small agencies assigned a senior agency official for privacy who is responsible for ensuring compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information by programs and information systems. Specifically, five of the six agencies had assigned an agency official with overall agency-wide responsibility for information privacy issues, while one agency had not. One of the agencies designated a Chief Privacy Officer, while officials from three other agencies stated that other employees or officers, specifically the Chief Operating Officer, the General Counsel, or the Chief Information Officer, were designated to perform the duties of a privacy officer. The fifth agency designated its Management and Program Officer as the agency's privacy official in 2014. The sixth agency, according to an agency official, did not have many full-time employees and had not identified an agency official responsible for privacy.

Incomplete implementation of privacy requirements by five of the six selected agencies may place PII in their systems at risk. The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information.

In a separate report for limited official use only, we are providing specific details on the weaknesses in the five selected agencies' implementation of privacy requirements.

OMB and DHS Offer Guidance to Agencies, but Oversight and Assistance for Small Agencies Needs Improvement

While OMB and DHS have various responsibilities in overseeing federal agencies' implementation of information security and privacy requirements, their oversight of small agencies has been limited. Specifically, OMB and DHS are not overseeing all small agencies' implementation of cybersecurity and privacy requirements. Moreover, OMB is not reporting small agencies' performance metrics for privacy in its annual FISMA report to Congress.

OMB and DHS have provided a variety of guidance and services to assist agencies in meeting security and privacy requirements, including a recently launched DHS initiative aimed at improving small agencies' cybersecurity. However, the agencies in our review have faced challenges in using the guidance and services, and additional efforts could better position smaller agencies to take advantage of guidance and services offered.

OMB and DHS Are Not Overseeing All Small Agencies on Information Security and Privacy Implementation

FISMA, the Privacy Act, and the E-Government Act include provisions that require OMB to oversee the implementation of the various information security and privacy requirements at all federal agencies. FISMA requires that OMB develop and oversee the implementation of policies, standards, and guidelines on information security at executive branch agencies and annually report to Congress on agencies' compliance with the act. The Privacy Act gives OMB responsibility for developing guidelines and providing "continuing assistance to and oversight of" agencies' implementation of the act. The E-Government Act of 2002 also assigns OMB responsibility for developing PIA guidance and ensuring agency implementation of the privacy impact assessment requirement. Since 2010, DHS has assisted OMB in overseeing executive branch agencies' compliance with FISMA, overseeing cybersecurity operations, and providing related assistance.[26] DHS cybersecurity oversight activities have also included privacy-related matters initiated by OMB in its continuing oversight of the implementation of the Privacy Act and the E-Government Act.

In overseeing small agencies' implementation of information security and privacy requirements, OMB and DHS have instructed the agencies to

[26] OMB memorandum M-10-28 (July 6, 2010) assigned DHS primary responsibility for the operational aspects of cybersecurity, subject to OMB oversight in accordance with FISMA.

report annually on a variety of metrics, which are used to gauge implementation of the information security programs and privacy requirements established by the various acts.[27] The metrics cover areas such as risk management, security training, remediation programs, and contingency planning. Over time, these metrics have evolved to include administration priorities[28] and baseline metrics[29] intended to improve oversight of FISMA implementation and federal information security. To report on the annual metrics, all federal agencies use an interactive data collection tool called CyberScope.

In its 2013 annual report to Congress on agencies' implementation of FISMA, OMB reported that small agencies improved their implementation of FISMA capabilities from fiscal year 2012 to fiscal year 2013. For example, in providing security awareness training to users, small agencies increased from 85 percent in fiscal year 2012 to 96 percent in fiscal year 2013. Another area of improvement noted was the capability for controlled incident detection: small agencies increased from 53 percent in fiscal year 2012 to 69 percent in fiscal year 2013. In addition, the number of small agencies reporting to OMB increased from 50 in fiscal year 2012 to 57 in fiscal year 2013.

However, as of March 2013, 55 of 129 small agencies registered to use CyberScope had never reported to OMB on the implementation of their information security programs. Further, one of the agencies in our review has never registered to use CyberScope or reported to OMB. The other agency, although initially registering to use CyberScope when it was first developed, never submitted its annual report and last reported to OMB in 2008.

[27] FISMA reporting instructions require that chief information officers submit monthly data feeds to CyberScope and report on a quarterly basis, and that inspectors general and senior agency officials for privacy report on an annual basis.

[28] The three administration priority areas for strengthening federal cybersecurity are (1) the Trusted Internet Connections initiative, (2) continuous monitoring of federal information systems, and (3) strong authentication.

[29] Baseline metrics include areas such as: tracking software assets, tracking hardware assets, and percentage of network boundary devices assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities, among others.

According to DHS officials, they report to OMB on which agencies met or did not meet the annual reporting requirement. Further, the list of agencies DHS reports on is limited to those that have registered for CyberScope. DHS officials also stated that reminders are sent to agencies about CyberScope reporting dates. However, DHS officials stated they have no mechanism in place to force agencies to comply with the annual reporting requirement. Establishing a mechanism, such as publishing a list of agencies not meeting the annual reporting requirements, could lead to greater transparency and compliance.

With regard to privacy oversight, OMB did not include in its 2013 report to Congress small agencies' performance in implementing privacy requirements, despite collecting this information.[30] Rather, privacy information was only included for larger agencies. According to OMB officials, privacy data are collected for all agencies through various methods, in addition to CyberScope reporting. These include, for example, E-Government Act section 208 reviews, reviews of system of records notices, and computer matching agreements. OMB officials further stated that it is up to agencies to adhere to privacy requirements and official guidance. However, as discussed earlier, three of the selected agencies in our review had not met privacy requirements. Including data on small agencies' implementation of privacy requirements in OMB's annual report to Congress could provide additional transparency and oversight.

OMB and DHS Provide Information Security and Privacy Guidance and Services to Federal Agencies, but Small Agencies Face Challenges in Using Them

OMB has provided guidance to federal agencies, including small agencies, on information security and privacy. Specifically, OMB has issued several memorandums intended to guide agencies in implementing FISMA, E-Government Act, and Privacy Act requirements, as well as other cybersecurity and privacy guidance intended to address shortcoming in federal systems and privacy requirements. Table 3 lists examples of key information security and privacy guidance issued by OMB.

[30] OMB instructs all large and small federal agencies to report on a set of privacy metrics. It does not require micro agencies to report on privacy metrics.

Table 3: Examples of OMB Information Security and Privacy Guidance to Federal Agencies

Title	Description
Information security implementing guidance	
OMB M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)* (Aug. 11, 2008)	Requires agencies to use validated security software to provide baseline system security settings.
OMB M-09-32, *Update on the Trusted Internet Connections Initiative* (Sept. 17, 2009)	Provides guidance on the Trusted Internet Connections (TIC) initiative to reduce internet access points and requests updates to agencies' plans of action and milestones for meeting TIC requirements.
OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management* (Nov. 18, 2013)	Provides instructions for meeting the agency's reporting requirements under FISMA and reporting instructions on the agency's privacy management program.
Privacy implementing guidance	
OMB, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 FR 28948 (July 9, 1975)	Defines responsibilities for implementing the Privacy Act of 1974, including the issuance of system of records notices.
OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 30, 2003)	Provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, including requirements for conducting privacy impact assessments for electronic information systems and collections.
OMB M-05-08, *Designation of Senior Agency Officials for Privacy* (Feb. 11, 2005)	Directs executive departments and agencies to identify the senior official who has overall agency-wide responsibility for information privacy issues.
OMB M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006)	Requires each agency senior official for privacy to conduct a review of agency policies and processes, and take corrective action as appropriate to ensure the agency has adequate safeguards to prevent the misuse of or unauthorized access to personally identifiable information (PII).
OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007)	Requires agencies to take several actions to protect PII, including reviewing and reducing the volume of PII, ensuring the implementation of security policy and National Institute of Standards and Technology guidance, and reporting all security incidents involving PII to United States Computer Emergency Readiness Team within 1 hour.

Source: GAO based on OMB guidance. | GAO-14-344

In addition to guidance, according to OMB officials, OMB regularly works with all agencies to discuss implementation of privacy requirements, both directly and through Chief Information Officer Council meetings. The Privacy Committee of the council is one mechanism used to communicate with agencies. According to OMB officials, agencies with a senior agency official for privacy are invited to attend these meetings, and small agencies may also participate. Further, OMB officials stated that they have separate meetings with small agencies, as appropriate. For example, according to OMB officials, their staff recently gave a detailed talk on privacy requirements to the Small Agency Council—General Counsel Forum.

Since 2010, DHS has had responsibilities in accordance with an OMB memorandum for overseeing and assisting federal agency efforts to provide adequate, risk-based, and cost-effective cybersecurity. Its activities have also included a number of privacy-related matters that assist OMB in carrying out its privacy oversight responsibilities. In undertaking these activities, DHS offers a variety of services to assist all federal agencies with implementing aspects of their information security and privacy programs (see table 4).

Table 4: Examples of Department of Homeland Security Services Available to Federal Agencies

Service	Description
Coordination of Cyber Security Incident Mitigation	Provides agencies with mitigation recommendations for cyber incidents. Also serves as a focal point for disseminating cyber threat and vulnerability analysis.
Security Awareness and Training	Provides common suites of information systems security training products and services for agencies, such as general security awareness training services and role-based security training.
Situational Awareness and Incident Response	Provides access to blanket purchase agreements to procure information security products and services related to federal enterprise awareness and incident response capabilities.
Risk Management Framework Assistance	Facilitates agencies' use of shared service centers for risk management framework solutions to improve the quality of service and reduce the cost of completing security assessments and authorizations.
Operational Assurance	Coordinates with agencies to conduct assessments to validate technical capabilities (tools and technologies) as well as operational readiness of people, processes, and security program maturity.
Risk Evaluation	Conducts system assessments that combine national threat and vulnerability information with data collected through onsite testing activities at federal agencies to provide the agency with tailored risk analysis reports and remediation recommendations based on risk.
National Cybersecurity Assessment & Technical Services	Leverages existing "best in breed" cybersecurity assessment methodologies, commercial best practices, and integration of threat intelligence that assist cybersecurity stakeholders with decision making and risk management guidance and recommendations.
Continuous Diagnostics & Mitigation program	Provides federal agencies with capabilities and tools to enable near real-time information on the state of agency networks to help identify and mitigate flaws in a timely manner.
Privacy Workshop and Guidance	Conducts privacy compliance workshops for federal agencies. DHS also publishes PIAs and system of record notices on its website as examples of privacy risk mitigations.

Source: GAO analysis based on agency documentation. | GAO-14-344

According to DHS, four of the six small agencies in our review used some services offered by the department in fiscal years 2012 and 2013. For example,

- DHS hosted advisory events in fiscal year 2012 for chief information officers of small agencies. These events covered topics such as continuous monitoring, FISMA, and insider threat briefings, among others. According to DHS officials, two general Chief Information Security Officer (CISO) Advisory Council events were held in fiscal year 2013. Small agencies attended these events. The focus of current events has moved to the Continuous Diagnostics and Mitigation Exercise Evaluation Guide meetings. This is due to the focus on continuous monitoring mandated by OMB. According to DHS officials, this was a natural transition as departments and agencies had more interest in learning about Continuous Diagnostics and Mitigation than in some of the other initiatives.
- Four of the six agencies in our review used a DHS-offered service to seek clarification and ask questions regarding FISMA issues.
- Two of the six agencies in our review participated in the National Cybersecurity Assessment and Technical Services for 2013.
- DHS is working with one agency in our review on recruiting and retaining cybersecurity expertise, providing additional information on insider threats and threat awareness programs, and obtaining clarification on CyberScope reporting.
- DHS is working with another agency in our review on its risk and vulnerability assessment, remediation strategies, and continuous monitoring policy development.
- One agency in our review participated in the privacy workshop.

Selected Agencies Face Challenges in Using Guidance

While OMB and DHS have provided agencies with guidance through their website, workshops, OMB's MAX portal,[31] and e-mail distribution lists, the six agencies in our review faced challenges with using the guidance. The following are examples of challenges in using OMB and DHS guidance identified by the small agencies we reviewed:

- OMB guidance directs agencies to use NIST guidance. However, according to agency officials in our review, since some smaller agencies do not have technical staff, they have difficulty interpreting and implementing the voluminous and technical publications issued by NIST.
- Two of the six agencies were either not aware of privacy guidance that is available or thought that the agency was not responsible for

[31] OMB uses the MAX Information System to collect, validate, analyze, model, collaborate with agencies on, and publish information relating to its government-wide management and budgeting activities.

applying the guidance. OMB and DHS did not provide evidence that they had reached out to all small agencies. As a result, it is not clear whether the six selected agencies were notified of issued privacy guidance. According to OMB officials, due to the large decentralized nature of the federal government, the opportunities to reach out to all federal agencies, whether large or small, are limited. Consequently, OMB distributes its guidance documents to a broad group and posts them on its website for easy access.

Selected Agencies Face Difficulties with Using Services

Similarly, while OMB and DHS offered chief information security officer advisory councils, chief information officer meetings for small agencies, and privacy workshops to all federal agencies, the six small agencies in our review faced challenges with attending. The following are examples of challenges the small agencies in our review identified:

- According to agency officials, the meetings that were held focused on cybersecurity issues faced by large agencies. Small agencies do not face the same technical issues and may not have the same capabilities, resources, personnel, and/or expertise as larger agencies to implement necessary cybersecurity requirements.
- Agency officials also stated that, since smaller agencies have fewer cybersecurity staff, they may not be available to attend meetings held by DHS.
- An official at one agency stated that when meetings require security clearances to attend, smaller agencies are unable to attend since their staff does not have available funds or a need to obtain the necessary clearances.
- Agency officials also noted they were not always made aware of meetings held by OMB or DHS, including chief information security officer advisory councils, small agency meetings, and privacy workshops.

During the course of our review, in December 2013, DHS established the Small & Micro-Agency Cybersecurity Support initiative. The initiative is intended to provide support to small agencies for implementing and improving cybersecurity programs. Through this initiative, DHS intends to provide IT security planning assistance and cybersecurity support to small agencies within the federal civilian executive branch. The support is focused on agencies that are attempting to enhance their cybersecurity posture but currently do not have the capabilities, resources, personnel, and/or expertise to implement necessary requirements.

In January 2014, DHS held a Small & Micro-Agency Cybersecurity workshop intended to inform small agencies on the various services offered to help them implement and improve their cybersecurity programs. For this workshop DHS contacted agencies from the small agency Chief Information Security Officer (CISO) Advisory Council events. At the workshop, DHS provided a discussion of

- its initiative providing support to small agencies;
- the Continuous Diagnostics & Mitigation program;
- options and strategies for implementing the Trusted Internet Connections mandate;
- blue teams, red teams,[32] assessments, outcomes, and solutions;
- US-CERT capabilities and incident reporting procedures at federal agencies; and
- fiscal year 2014 and 2015 challenges.

As of February 2014, five agencies were participating in a pilot program for the Small and Micro-Agency Cybersecurity Support Initiative, including two of the six agencies from our review. As DHS continues with the pilot program, developing services and guidance that address the challenges discussed in this report could further assist small agencies. For example, guidance and assistance targeted to these agencies' environments could help them improve the implementation of their security programs and various privacy requirements.

Conclusions

Securing information systems and protecting the privacy of personal information is a challenge for the small agencies we reviewed. Although these agencies have implemented elements of an information security program and privacy requirements, weaknesses put agencies' information systems and the information they contain at risk of compromise. Addressing these weaknesses is essential for these agencies to protect their information and systems. Without adequate safeguards, the small agencies we reviewed will remain vulnerable to individuals and groups with malicious intentions, who may obtain sensitive information, commit

[32] According to NIST, blue teams and red teams are typically responsible for defending (blue team) and emulating an attack (red team) on the enterprise's use of information systems. Both teams' objective is to improve enterprise information assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the blue team) in an operational environment. The term "blue team" is also used for a group that conducts independent operational network vulnerability evaluations and provides mitigation techniques to customers.

fraud, disrupt operations, or launch attacks against other computer systems and networks.

Moreover, while OMB and DHS have continued to oversee agencies' information security programs and implementation of privacy requirements and provide guidance and services, they have not consistently ensured that all small agencies have reported on their compliance with security and privacy requirements, making it more difficult to accurately assess the extent to which agencies are effectively securing their information and systems. Additionally, those agencies that were aware of the guidance and services have been challenged with using it. Without the additional assistance, oversight, and collection of security and privacy information for the selected small agencies, OMB and DHS may be unaware of the agencies' implementation of requirements and the assistance that is needed.

Recommendations for Executive Action

To improve the consistency and effectiveness of government-wide implementation of information security programs and privacy requirements at small agencies, we recommend that the Director of OMB include in the annual report to Congress on agencies' implementation of FISMA

- a list of agencies that did not report on implementation of their information security programs, and
- information on small agencies' implementation of privacy requirements.

In addition, we recommend that the Secretary of Homeland Security, as part of the department's Small & Micro-Agency Cybersecurity Support Initiative, develop services and guidance targeted to small and micro agencies' environments.

In a separate report with limited distribution, we are also making detailed recommendations to the selected agencies in our review to correct weaknesses identified in their information security and privacy programs.

Agency Comments and Our Evaluation

We provided a draft of this report to the six agencies selected for our review, as well as to DHS, the Office of Personnel Management, and OMB. We received written responses from DHS, the Federal Trade Commission, and the James Madison Memorial Foundation. These comments are reprinted in appendices II through IV. We received e-mail comments from OMB, the National Endowment for the Humanities, and the International Boundary Commission, United States and Canada. The other three agencies had no comments on our report.

The audit liaison for OMB responded via e-mail on June 10, 2014, that OMB generally agreed with our recommendations and provided technical comments. We incorporated them as appropriate.

In its written comments (reproduced in appendix II), DHS concurred with our recommendation and identified actions it has taken or plans to take to implement our recommendation. For example, as part of its fiscal year 2014 hiring plan, the National Protection and Programs Directorate's Office of Cybersecurity and Communications is establishing and expanding a new federal customer service unit within the United States Computer Emergency Readiness Team to better understand the circumstances and needs of the various federal civilian departments and agencies, including small and micro agencies. According to DHS, the customer service unit will help develop and improve services and guidance that address the particular needs of agencies with 6,000 full-time employees or less. According to DHS, these actions will be completed by April 30, 2015.

In its written comments (reproduced in app. III), the Federal Trade Commission acknowledged that improvements can be made in aspects of its information security program and described steps it has taken or plans to take to address weaknesses we identified.

In its written comments (reproduced in app. IV), the James Madison Memorial Foundation reiterated that it is one of the smallest agencies in the federal government, with only three full-time employees and one half-time employee, and that it had operated since November 2010 with the understanding that the agency was granted an exemption from FISMA by OMB officials. However, the agency stated that it plans to take the necessary actions to conform to FISMA requirements.

The Chief Information Officer for the National Endowment for the Humanities provided comments via e-mail on June 6, 2014. He discussed the usefulness of the report contents and noted that it was very much needed. In addition, he noted that GAO's report highlights the lack of compliance with reporting requirements by small agencies and that these agencies may be struggling to meet all requirements. He further commented that large agencies, unlike small agencies, have dedicated IT staff and that there should not be a "one size fits all" set of requirements for all federal agencies. However, while smaller federal agencies may not have dedicated IT staff, we believe federal agencies, large or small, should perform an assessment of their risks and implement appropriate safeguards to reduce risk to an acceptable level. He also provided technical comments, which we incorporated as appropriate.

The Acting Commissioner for the International Boundary Commission, United States and Canada, provided comments via e-mail on June 5, 2014. The Acting Commissioner stated that he disagreed with our statement that all computer equipment within the agencies reviewed contained classified or sensitive information. However, our report does not state this; rather, it discusses the selected agencies' actions to implement federal information security and privacy requirements. We believe our characterization of the weaknesses identified is accurate as of the time of our review.

The Deputy Chief Risk Officer for the Federal Retirement Thrift Investment Board and the audit liaisons for the Office of Personnel Management and National Capital Planning Commission responded via e-mail that these agencies did not have any comments on the draft report.

We are sending copies of this report to the Secretary of Homeland Security, the Director of the Office of Management and Budget, and the heads of the six agencies we reviewed. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Nabajyoti Barkakati

Dr. Nabajyoti Barkakati
Chief Technologist

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the extent to which (1) selected small agencies are implementing federal information security and privacy laws and policies, and (2) the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) are overseeing and assisting small agencies in implementing their information security and privacy programs.

To assess how small agencies were implementing federal information security and privacy laws, we selected six agencies for review. We selected these six agencies by creating a list of all small, micro, and independent regulatory[1] agencies using definitions from OMB Circular A-11, CyberScope,[2] the Paperwork Reduction Act, USA.gov, and Office of Personnel Management information. We used OMB's definition of small agencies as agencies with fewer than 6,000 employees and micro agencies as agencies having fewer than 100 employees. We excluded the 24 agencies covered by the Chief Financial Officers Act,[3] agencies that are part of the Executive Office of the President, agencies from the

[1] Independent regulatory agencies, as defined by the Paperwork Reduction Act, include the Board of Governors of the Federal Reserve System, Commodity Futures Trading Commission, Consumer Product Safety Commission, Federal Communications Commission, Federal Deposit Insurance Corporation, Federal Energy Regulatory Commission, Federal Housing Finance Board, Federal Maritime Commission, Federal Trade Commission, Interstate Commerce Commission, Mine Enforcement Safety and Health Review Commission, National Labor Relations Board, Nuclear Regulatory Commission, Occupational Safety and Health Review Commission, Postal Rate Commission, Securities and Exchange Commission, and any other similar agency designated by statute as a federal independent regulatory agency or commission. The following agencies no longer exist: the Federal Housing Finance Board, Interstate Commerce Commission, Mine Enforcement Safety and Health Review, and Postal Rate Commission. The Federal Housing Finance Board is now the Federal Housing Finance Agency, and the Postal Rate Commission is the Postal Regulatory Commission.

[2] CyberScope is an interactive data collection tool that has the capability to receive data feeds on a recurring basis to assess the security posture of a federal agency's information infrastructure. Agencies are required to use this tool to respond to reporting metrics.

[3] The Chief Financial Officers Act agencies are the executive branch agencies listed at 31 U.S.C. §901(b). They 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; National Aeronautics and Space Administration; General Services Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

intelligence community, and agencies whose financial statements are audited annually by GAO.

We selected the agencies by organizing the list of small agencies into five primary areas: (1) boards, commissions, and corporations reporting through CyberScope; (2) boards, commissions, and corporations not reporting through CyberScope; (3) independent regulatory agencies; (4) memorial, arts, foundations, and administrative agencies reporting through CyberScope; and (5) memorial, arts, foundations, and administrative agencies not reporting through CyberScope. Using a randomly generated number, we selected one agency from each area. The five resulting agencies were the (1) Federal Trade Commission; (2) International Boundary Commission, United States and Canada; (3) James Madison Memorial Fellowship Foundation; (4) National Capital Planning Commission; and (5) National Endowment for the Humanities. We selected the sixth agency, the Federal Retirement Thrift Investment Board, because it had experienced a significant data breach involving personally identifiable information. Due to the sensitive nature of the information discussed, throughout the report we do not refer to the six agencies by name.

To identify agency, OMB, and National Institute of Standards and Technology (NIST) responsibilities for agency information security and privacy, we reviewed and analyzed the provisions of the E-Government Act of 2002, Federal Information Security Management Act (FISMA) of 2002, and the Privacy Act of 1974. At each of the six agencies, we interviewed senior information security program and privacy staff, observed controls, and conducted technical reviews to gain an understanding of the agency, the information technology environment, and the information security and privacy programs.

To evaluate agencies' implementation of their information security responsibilities, we reviewed and analyzed agency documentation and compared it to provisions in FISMA and NIST guidance. We reviewed information security policies and procedures, information technology security-related audit reports, CyberScope data (where available), and inspector general reports for work conducted in fiscal years 2011, 2012, and 2013. To evaluate the privacy programs at each agency, we assessed whether the six agencies had established plans for privacy protections and conducted impact assessments for systems containing personally identifiable information, as required by the E-Government Act. We assessed whether the six agencies had issued system of records notices for each system containing personally identifiable information, as called for by the Privacy Act. We reviewed OMB memorandum M-03-22 and NIST Special Publication 800-122 to select privacy elements required of federal agencies. We then reviewed and analyzed documents from the selected agencies, including privacy policies and procedures, to determine whether they adhered to the requirements set forth in OMB and NIST guidance. We also interviewed agency officials to determine what assistance they had requested and received from OMB and areas where it would have been beneficial to receive additional assistance. Because of the small number of agencies reviewed, our findings are not representative of any population of small agencies and our results only apply to the six selected agencies and to their selected systems.

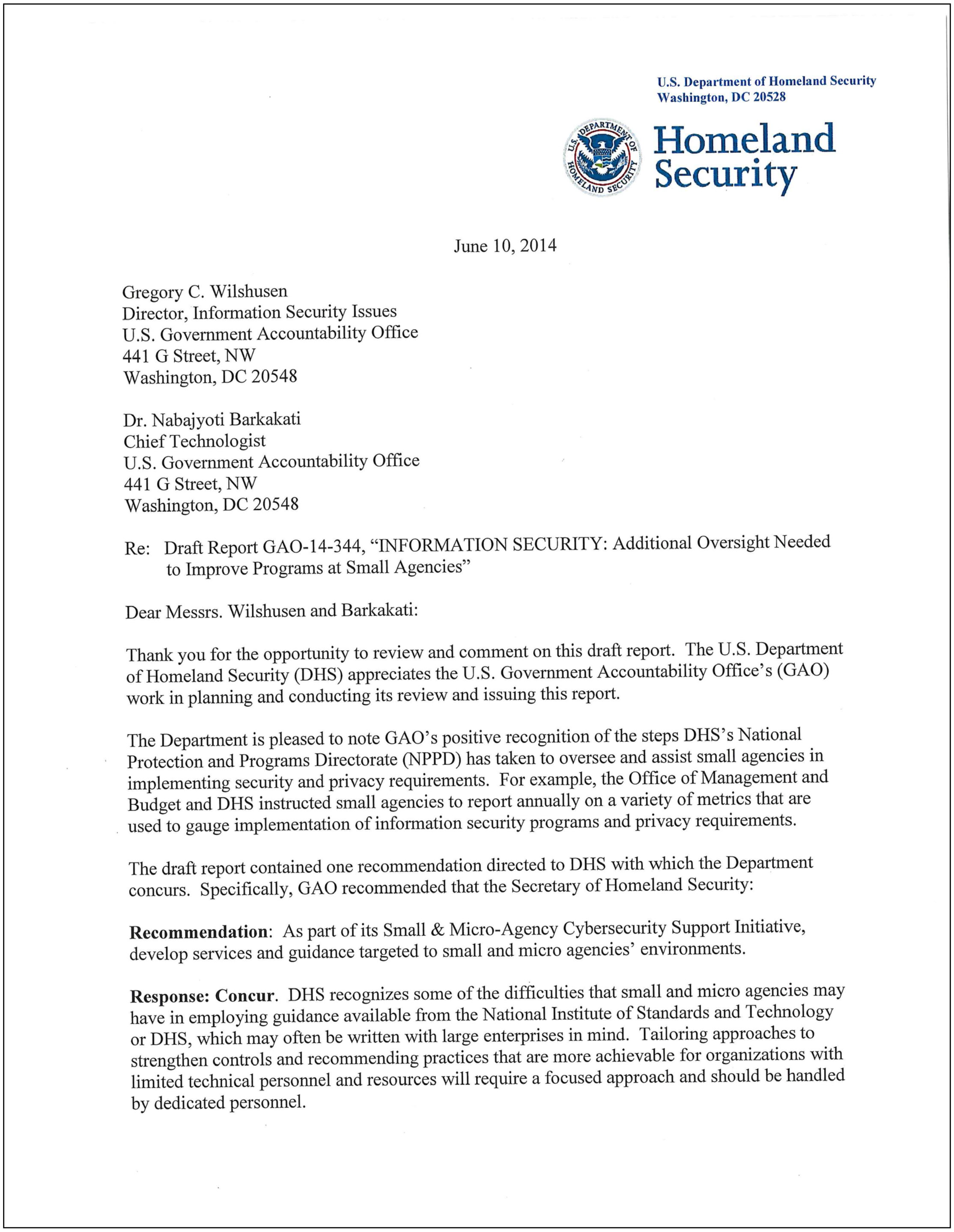
To determine the extent to which DHS and OMB are overseeing and assisting small agencies in implementing information security program requirements, we reviewed OMB's guidance to determine the Department of Homeland Security's responsibilities. We reviewed and analyzed DHS's and OMB's policies, procedures, and plans related to security to determine the level of guidance DHS provided to small federal agencies. We reviewed DHS's and OMB's fiscal years 2011, 2012, and 2013 guidance for agency reporting on FISMA and compared it to FISMA requirements. Additionally, we reviewed the six agencies' fiscal years 2011 and 2012 FISMA data submissions to determine the extent to which DHS uses data to assist agencies in effectively implementing information security program requirements. We interviewed DHS officials in the Office of Cybersecurity and Communications, U.S. Computer Emergency Readiness Team (US-CERT), Federal Network Resilience Division, and other DHS entities. We reviewed and analyzed documentation that supported agency assistance requests, technical alerts, after-action reports, and other available documentation to determine the extent to which US-CERT tracks and provides assistance to small agencies. We conducted interviews with OMB officials based on the documentation and information provided. We did not evaluate the implementation of DHS's FISMA-related responsibilities assigned to it by OMB.

To evaluate the extent to which DHS and OMB are overseeing and assisting small agencies in implementing privacy laws and policies, we reviewed OMB-issued guidance on Privacy Impact Assessments and each selected agency's privacy notices. Additionally, we reviewed DHS's privacy guidance. We met with DHS and OMB officials to determine the actions taken to provide assistance and oversight to federal agencies.

To determine the reliability and accuracy of the data, we obtained and analyzed data from each agency that addressed the security and privacy internal controls of the systems used to collect the data. Specifically, we analyzed data regarding access controls, incident reporting, security awareness training, change management, and remediation of weaknesses. In addition, we interviewed agency officials responsible for the collection and reporting of the data. Based on these procedures, we determined the data were sufficiently reliable for the purpose of this report.

We conducted this performance audit from January 2013 to June 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.

Appendix II: Comments from the Department of Homeland Security



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

Homeland Security

June 10, 2014

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

Dr. Nabajyoti Barkakati
Chief Technologist
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-14-344, "INFORMATION SECURITY: Additional Oversight Needed to Improve Programs at Small Agencies"

Dear Messrs. Wilshusen and Barkakati:

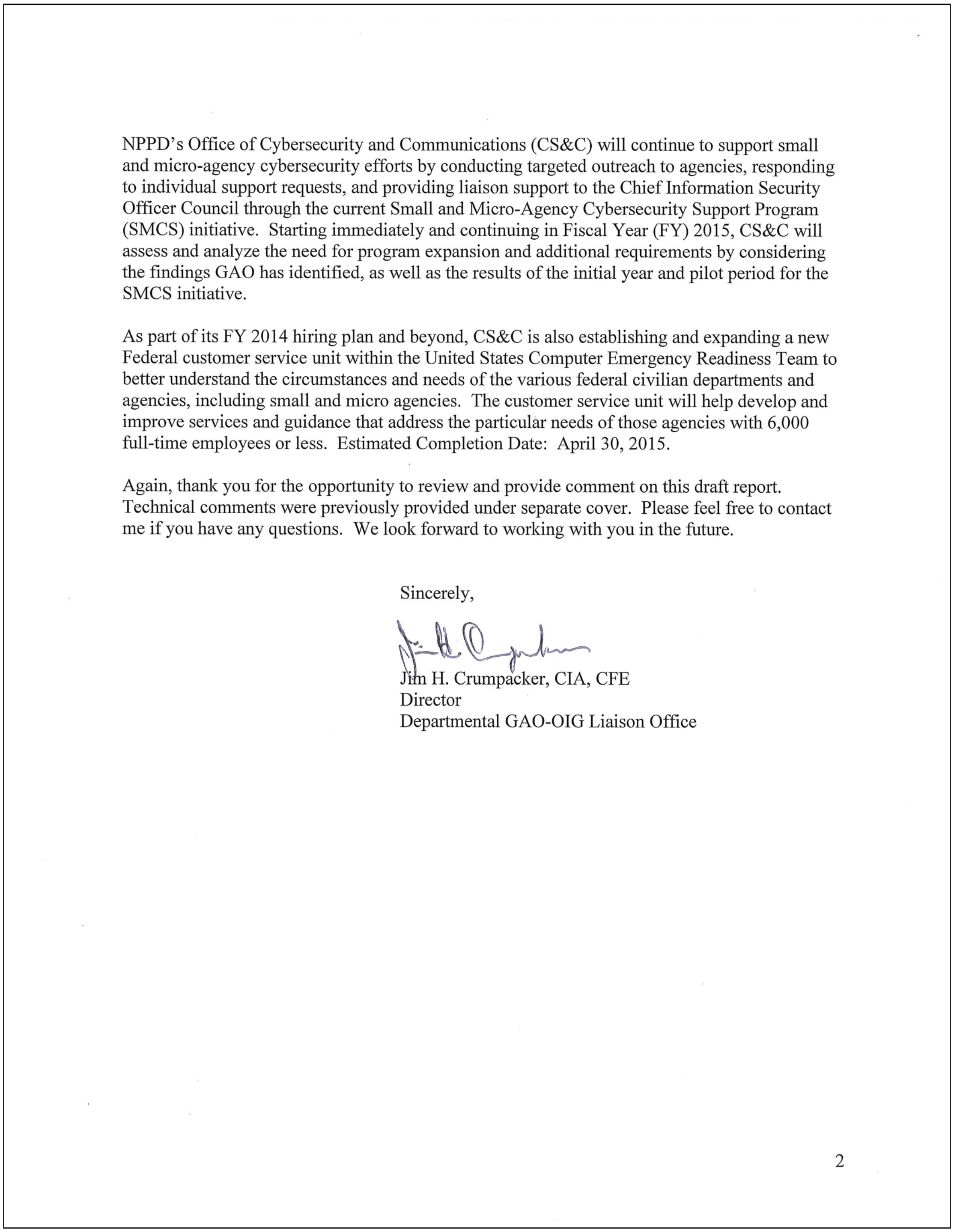
Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive recognition of the steps DHS's National Protection and Programs Directorate (NPPD) has taken to oversee and assist small agencies in implementing security and privacy requirements. For example, the Office of Management and Budget and DHS instructed small agencies to report annually on a variety of metrics that are used to gauge implementation of information security programs and privacy requirements.

The draft report contained one recommendation directed to DHS with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation: As part of its Small & Micro-Agency Cybersecurity Support Initiative, develop services and guidance targeted to small and micro agencies' environments.

Response: Concur. DHS recognizes some of the difficulties that small and micro agencies may have in employing guidance available from the National Institute of Standards and Technology or DHS, which may often be written with large enterprises in mind. Tailoring approaches to strengthen controls and recommending practices that are more achievable for organizations with limited technical personnel and resources will require a focused approach and should be handled by dedicated personnel.



NPPD's Office of Cybersecurity and Communications (CS&C) will continue to support small and micro-agency cybersecurity efforts by conducting targeted outreach to agencies, responding to individual support requests, and providing liaison support to the Chief Information Security Officer Council through the current Small and Micro-Agency Cybersecurity Support Program (SMCS) initiative. Starting immediately and continuing in Fiscal Year (FY) 2015, CS&C will assess and analyze the need for program expansion and additional requirements by considering the findings GAO has identified, as well as the results of the initial year and pilot period for the SMCS initiative.

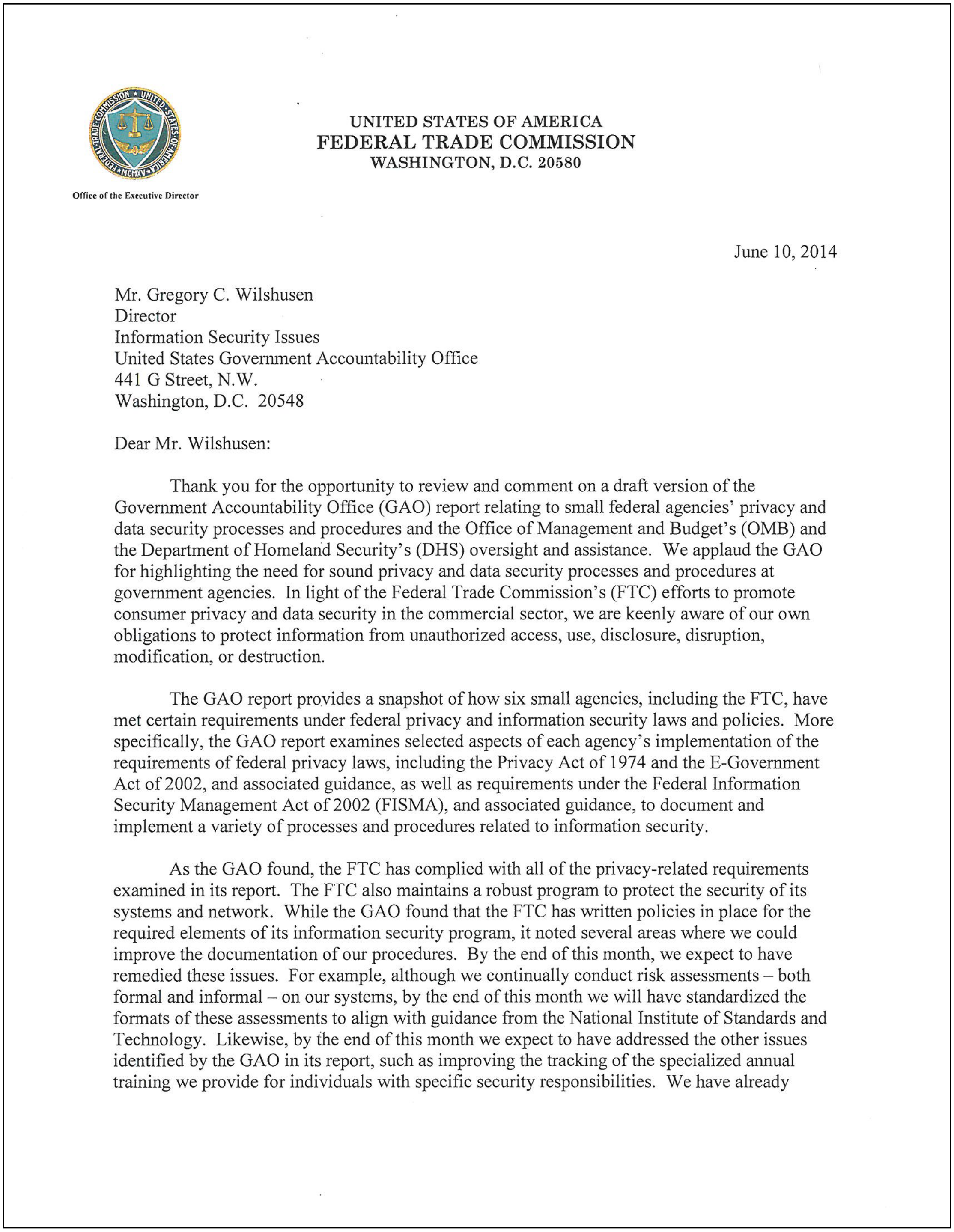
As part of its FY 2014 hiring plan and beyond, CS&C is also establishing and expanding a new Federal customer service unit within the United States Computer Emergency Readiness Team to better understand the circumstances and needs of the various federal civilian departments and agencies, including small and micro agencies. The customer service unit will help develop and improve services and guidance that address the particular needs of those agencies with 6,000 full-time employees or less. Estimated Completion Date: April 30, 2015.

Again, thank you for the opportunity to review and provide comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

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

Appendix III: Comments from the Federal Trade Commission



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Executive Director

June 10, 2014

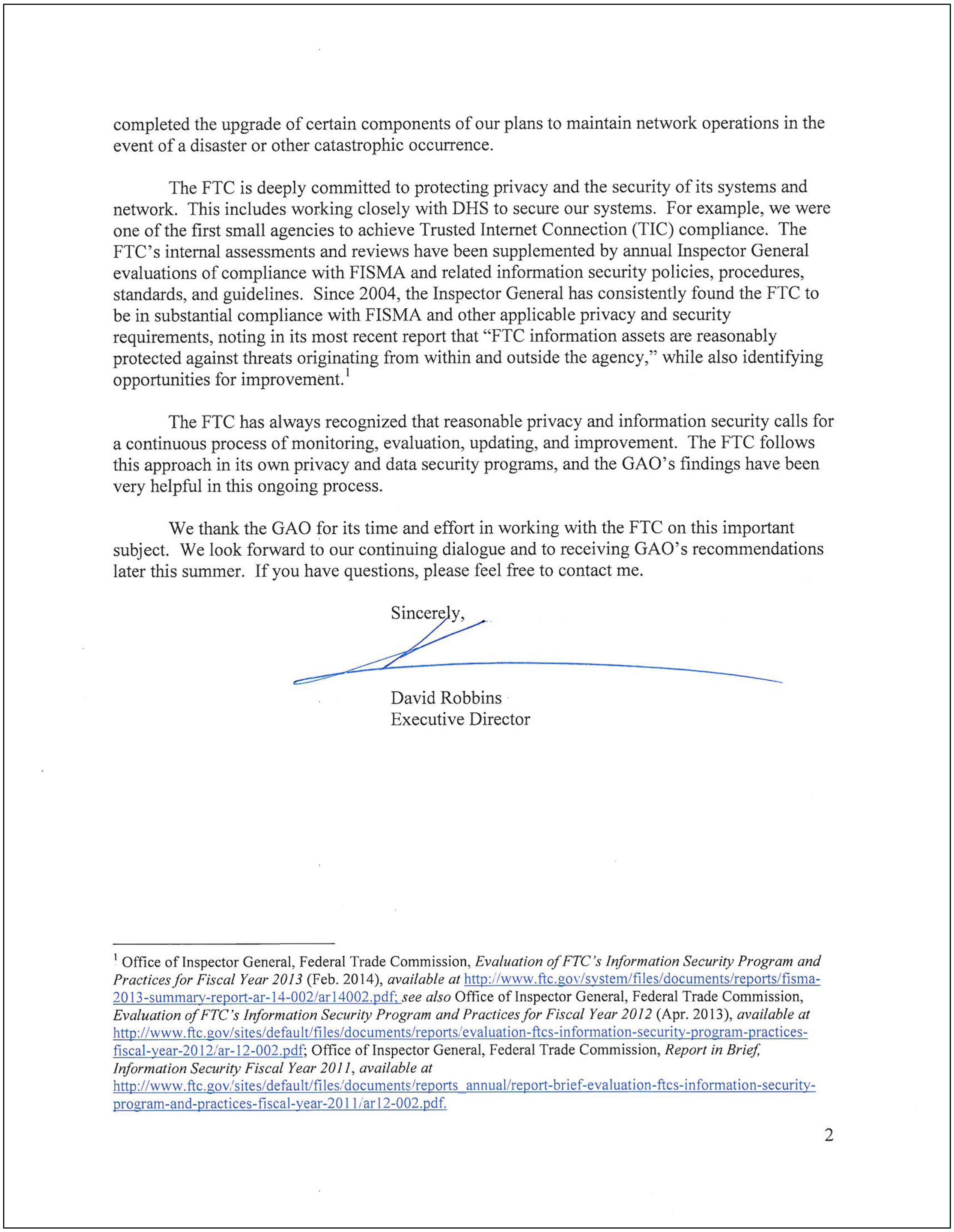
Mr. Gregory C. Wilshusen
Director
Information Security Issues
United States Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on a draft version of the Government Accountability Office (GAO) report relating to small federal agencies' privacy and data security processes and procedures and the Office of Management and Budget's (OMB) and the Department of Homeland Security's (DHS) oversight and assistance. We applaud the GAO for highlighting the need for sound privacy and data security processes and procedures at government agencies. In light of the Federal Trade Commission's (FTC) efforts to promote consumer privacy and data security in the commercial sector, we are keenly aware of our own obligations to protect information from unauthorized access, use, disclosure, disruption, modification, or destruction.

The GAO report provides a snapshot of how six small agencies, including the FTC, have met certain requirements under federal privacy and information security laws and policies. More specifically, the GAO report examines selected aspects of each agency's implementation of the requirements of federal privacy laws, including the Privacy Act of 1974 and the E-Government Act of 2002, and associated guidance, as well as requirements under the Federal Information Security Management Act of 2002 (FISMA), and associated guidance, to document and implement a variety of processes and procedures related to information security.

As the GAO found, the FTC has complied with all of the privacy-related requirements examined in its report. The FTC also maintains a robust program to protect the security of its systems and network. While the GAO found that the FTC has written policies in place for the required elements of its information security program, it noted several areas where we could improve the documentation of our procedures. By the end of this month, we expect to have remedied these issues. For example, although we continually conduct risk assessments – both formal and informal – on our systems, by the end of this month we will have standardized the formats of these assessments to align with guidance from the National Institute of Standards and Technology. Likewise, by the end of this month we expect to have addressed the other issues identified by the GAO in its report, such as improving the tracking of the specialized annual training we provide for individuals with specific security responsibilities. We have already



completed the upgrade of certain components of our plans to maintain network operations in the event of a disaster or other catastrophic occurrence.

The FTC is deeply committed to protecting privacy and the security of its systems and network. This includes working closely with DHS to secure our systems. For example, we were one of the first small agencies to achieve Trusted Internet Connection (TIC) compliance. The FTC's internal assessments and reviews have been supplemented by annual Inspector General evaluations of compliance with FISMA and related information security policies, procedures, standards, and guidelines. Since 2004, the Inspector General has consistently found the FTC to be in substantial compliance with FISMA and other applicable privacy and security requirements, noting in its most recent report that "FTC information assets are reasonably protected against threats originating from within and outside the agency," while also identifying opportunities for improvement.[1]

The FTC has always recognized that reasonable privacy and information security calls for a continuous process of monitoring, evaluation, updating, and improvement. The FTC follows this approach in its own privacy and data security programs, and the GAO's findings have been very helpful in this ongoing process.

We thank the GAO for its time and effort in working with the FTC on this important subject. We look forward to our continuing dialogue and to receiving GAO's recommendations later this summer. If you have questions, please feel free to contact me.

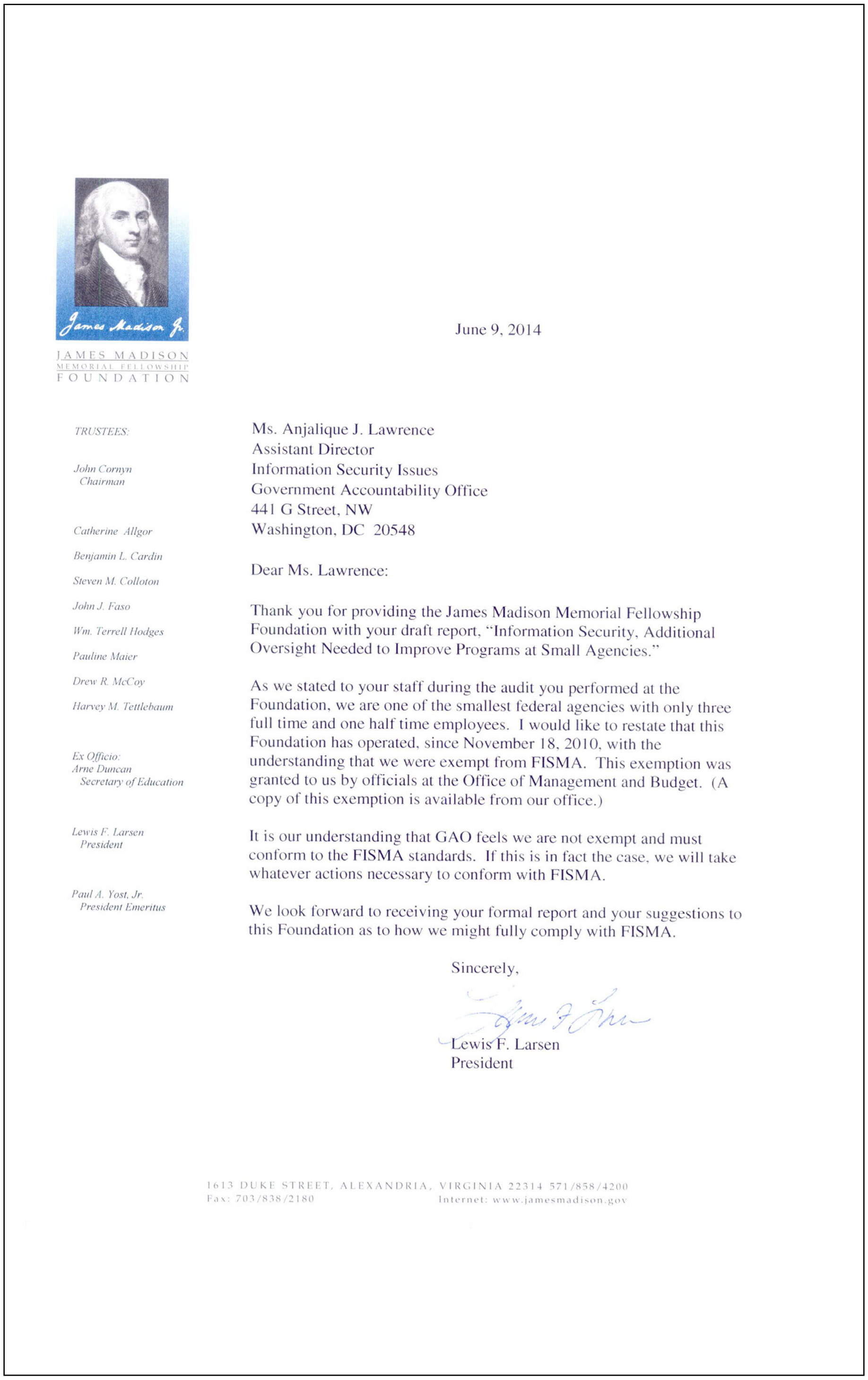
Sincerely,

David Robbins
Executive Director

[1] Office of Inspector General, Federal Trade Commission, *Evaluation of FTC's Information Security Program and Practices for Fiscal Year 2013* (Feb. 2014), *available at* http://www.ftc.gov/system/files/documents/reports/fisma-2013-summary-report-ar-14-002/ar14002.pdf; *see also* Office of Inspector General, Federal Trade Commission, *Evaluation of FTC's Information Security Program and Practices for Fiscal Year 2012* (Apr. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/evaluation-ftcs-information-security-program-practices-fiscal-year-2012/ar-12-002.pdf; Office of Inspector General, Federal Trade Commission, *Report in Brief, Information Security Fiscal Year 2011*, *available at* http://www.ftc.gov/sites/default/files/documents/reports_annual/report-brief-evaluation-ftcs-information-security-program-and-practices-fiscal-year-2011/ar12-002.pdf.

2

Appendix IV: Comments from the James Madison Memorial Fellowship Foundation



JAMES MADISON
MEMORIAL FELLOWSHIP
FOUNDATION

June 9, 2014

Ms. Anjalique J. Lawrence
Assistant Director
Information Security Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Lawrence:

Thank you for providing the James Madison Memorial Fellowship Foundation with your draft report, "Information Security, Additional Oversight Needed to Improve Programs at Small Agencies."

As we stated to your staff during the audit you performed at the Foundation, we are one of the smallest federal agencies with only three full time and one half time employees. I would like to restate that this Foundation has operated, since November 18, 2010, with the understanding that we were exempt from FISMA. This exemption was granted to us by officials at the Office of Management and Budget. (A copy of this exemption is available from our office.)

It is our understanding that GAO feels we are not exempt and must conform to the FISMA standards. If this is in fact the case, we will take whatever actions necessary to conform with FISMA.

We look forward to receiving your formal report and your suggestions to this Foundation as to how we might fully comply with FISMA.

Sincerely,

Lewis F. Larsen
President

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov
Dr. Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following made key contributions to this report: Edward Alexander, Jr., and Anjalique Lawrence (assistant directors), Cortland Bradford, Debra Conner, Rosanna Guerrero, Wilfred B. Holloway, Lee McCracken, David F. Plocher, Zsaroq Powe, Brian Vasquez, and Shaunyce Wallace.

(311302)

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.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, 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, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548