



August 2016

# FEDERAL CHIEF INFORMATION SECURITY OFFICERS

## Opportunities Exist to Improve Roles and Address Challenges to Authority

## Why GAO Did This Study

Federal agencies face an ever-increasing array of cyber threats to their information systems and information. To address these threats, FISMA 2014 requires agencies to designate a CISO—a key position in agency efforts to manage information security risks.

GAO was asked to review current CISO authorities. This report identifies (1) the key responsibilities of federal CISOs established by federal law and guidance and the extent to which federal agencies have defined the role of the CISO in accordance with law and guidance and (2) key challenges of federal CISOs in fulfilling their responsibilities. GAO reviewed agency security policies, administered a survey to 24 CISOs, interviewed current CISOs, and spoke with officials from OMB.

## What GAO Recommends

GAO is making 33 recommendations to 13 agencies to fully define the role of their CISOs in accordance with FISMA 2014. Twelve of the 13 agencies concurred with the recommendations addressed to them. One agency partially concurred or did not concur with the recommendations directed to it. GAO continues to believe that these recommendations are valid and should be implemented as discussed in this report. GAO also recommends that OMB issue guidance for clarifying CISOs' roles in light of identified challenges. OMB partially concurred with the recommendation. GAO maintains that action is needed as discussed further in the report.

View [GAO-16-686](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov).

# FEDERAL CHIEF INFORMATION SECURITY OFFICERS

## Opportunities Exist to Improve Roles and Address Challenges to Authority

### What GAO Found

Under the Federal Information Security Modernization Act of 2014 (FISMA 2014), the agency chief information security officer (CISO) has the responsibility to ensure that the agency is meeting the requirements of the law, including developing, documenting, and implementing the agency-wide information security program. However, 13 of the 24 agencies GAO reviewed had not fully defined the role of their CISO in accordance with these requirements. For example, these agencies did not always identify a role for the CISO in ensuring that security controls are periodically tested; procedures are in place for detecting, reporting, and responding to security incidents; or contingency plans and procedures for agency information systems are in place. Thus, CISOs' ability to effectively oversee these agencies' information security activities can be limited.

The 24 CISOs GAO surveyed identified challenges that limited their authority to carry out their responsibilities to oversee information security activities. These challenges can impact agencies' ability to effectively manage information security risk. The table below shows the factors that CISOs reported as being the most challenging to their authority.

**Extent to Which 24 Chief Information Security Officers Reported Factors as Challenging to Their Authority**

Factor	Large extent	Moderate extent	Small extent	Not at all	No response
Competing priorities between operations and security	6	12	4	2	0
Coordination with component organizations	5	8	4	5	2
Coordination with other offices	3	9	3	9	0
Availability of information from contractors	4	8	10	2	0
Oversight of indirect reports	6	6	6	6	0
Oversight of IT contractors	4	8	6	6	0
Placement in organizational hierarchy	5	5	5	9	0
Availability of information from component organizations	5	4	10	5	0

Source: GAO analysis of survey data. | GAO-16-686

The 24 CISOs also reported that other factors posed challenges to their abilities to carry out their responsibilities effectively, including difficulties related to having sufficient staff; recruiting, hiring, and retaining security personnel; ensuring that security personnel have appropriate expertise and skills; and a lack of sufficient financial resources. Several government-wide activities are under way to address many of these challenges. However, while the Office of Management and Budget (OMB) has a statutory responsibility under FISMA 2014 to provide guidance on information security in federal agencies, it has not issued such guidance addressing how agencies should ensure that officials carry out their responsibilities and personnel are held accountable for complying with the agency-wide information security program. As a result, agencies lack clarity on how to ensure that their CISOs have adequate authority to effectively carry out their duties in the face of numerous challenges.

---

# Contents

---

---

Letter		1
	Background	4
	Most Federal Agencies Defined the Role of the CISO in Accordance with Federal Law and Guidance	7
	Federal CISOs Identified Challenges to Their Authority That Limit Their Ability to Effectively Manage Agency-Wide Information Security Programs	26
	Conclusions	39
	Recommendations for Executive Action	40
	Agency Comments and Our Evaluation	40
Appendix I	Objectives, Scope, and Methodology	43
Appendix II	Recommendations to Departments and Agencies	46
Appendix III	Comments from the Department of Commerce	54
Appendix IV	Comments from the Department of Defense	56
Appendix V	Comments from the Department of Energy	62
Appendix VI	Comments from the Department of Health and Human Services	68
Appendix VII	Comments from the Department of Housing and Urban Development	70
Appendix VIII	Comments from the Department of the Interior	71

---

Appendix IX	Comments from the Department of Justice	72
Appendix X	Comments from the Department of State	74
Appendix XI	Comments from the Environmental Protection Agency	76
Appendix XII	Comments from the National Aeronautics and Space Administration	77
Appendix XIII	Comments from the U.S. Agency for International Development	78
Appendix XIV	Comments from the Social Security Administration	80
Appendix XV	GAO Contact and Staff Acknowledgments	81
Table	Table 1: Extent to Which 24 Agencies Defined the Role of Their Chief Information Security Officer	12
Figures	Figure 1: Extent to Which 24 Agency Chief Information Security Officers Identified Competing Priorities between Agency Operations and Information Security as Challenging	27
	Figure 2: Extent to Which 24 Agency Chief Information Security Officers Identified Coordination with Component Organizations and Other Offices as Challenging	28
	Figure 3: Extent to Which 24 Agency Chief Information Security Officers Identified Availability of Security-Related Information from Component Organizations and IT Contractors as Challenging	30

---

---

Figure 4: Extent to Which 24 Agency Chief Information Security Officers Identified Oversight of Indirect Reports and IT Contractors as Challenging	32
Figure 5: Extent to Which 24 Agency Chief Information Security Officers Identified Their Placement in the Agency Hierarchy as Challenging	34

---

---

## Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
Commerce	Department of Commerce
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
EPA	Environmental Protection Agency
FISMA 2002	Federal Information Security Management Act of 2002
FISMA 2014	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
Interior	Department of the Interior
ISSO	Information System Security Officer
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
POA&M	plan of action and milestones
SAISO	senior agency information security officer
SISO	senior information security officer
SP	Special Publication
SSA	Social Security Administration
State	Department of State
Treasury	Department of the Treasury
USAID	U.S. Agency for International Development
USDA	U.S. Department of Agriculture
VA	Department of Veterans Affairs

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



August 26, 2016

The Honorable Fred Upton  
Chairman  
Committee on Energy and Commerce  
House of Representatives

The Honorable Tim Murphy  
Chairman  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
House of Representatives

The widespread use of the Internet has changed the way that our government, our nation, and the rest of the world communicate and conduct business. While the benefits have been enormous, this connectivity—without effective cybersecurity—can also pose significant risks to computer systems and networks as well as to the critical operations and key infrastructures they support. Resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructures<sup>1</sup> could be disrupted, with potentially catastrophic effects. Accordingly, since 1997, we have designated information security as a government-wide high-risk area.<sup>2</sup> In 2003, we expanded this high-risk area to include computerized systems supporting our nation’s critical infrastructure.<sup>3</sup> In our 2015 High-Risk update,<sup>4</sup> we further expanded this

---

<sup>1</sup>Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. These critical infrastructures are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

<sup>2</sup>GAO, *High-Risk Series: Information Management and Technology*, [GAO/HR-97-9](#) (Washington, D.C.: Feb. 1, 1997) and *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

<sup>3</sup>See GAO, *High-Risk Series: An Overview*, [GAO/HR-97-1](#) (Washington, D.C.: Feb. 1, 1997) and *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: Jan. 1, 2003).

<sup>4</sup>See [GAO-15-290](#).

---

area to include protecting the privacy of personally identifiable information (PII).<sup>5</sup>

To address these challenges in the federal government, the Federal Information Security Management Act of 2002 (FISMA 2002),<sup>6</sup> and its successor, the Federal Information Security Modernization Act of 2014 (FISMA 2014),<sup>7</sup> require each agency in the executive branch to develop, document, and implement an information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.<sup>8</sup>

Nonetheless, our work and reviews by inspectors general have shown that federal agencies continue to have weaknesses in information security controls that place critical information and information systems used to support the operations, assets, and personnel of federal agencies at risk.

FISMA directs agency heads to delegate authority to ensure compliance with the law to agency chief information officers (CIO), who in turn are required to designate a senior agency information security officer to carry out the CIO's responsibilities.<sup>9</sup> These officials are generally referred to as chief information security officers (CISO).

Recognizing the importance of the CISO position in addressing the information security risks facing the federal government, you asked us to

---

<sup>5</sup>Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

<sup>6</sup>The Federal Information Security Management Act of 2002 was enacted as Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (Dec. 17, 2002).

<sup>7</sup>The Federal Information Security Modernization Act of 2014 was enacted as Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014). It updated and largely supersedes the very similar 2002 law, but retains many of the requirements for federal agencies' information security programs previously set by the 2002 law.

<sup>8</sup>Throughout this report, we will refer to the 2002 law as FISMA 2002 and the Federal Information Security Modernization Act of 2014 as FISMA 2014 when it is necessary to differentiate between them. We will use the term "FISMA" when referring to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

<sup>9</sup>44 U.S.C. § 3554(a)(3).



---

conduct a government-wide review of CISO authorities. Our objectives were to (1) identify the key responsibilities of federal CISOs established by federal law and guidance and determine the extent to which federal agencies have defined the role of the CISO in accordance with this law and guidance; and (2) describe key challenges of federal agency CISOs in fulfilling their responsibilities to ensure that agency-wide information security programs are developed, documented, and implemented.

To address these objectives, we reviewed relevant laws, National Institute of Standards and Technology (NIST) guidance, and Office of Management and Budget (OMB) guidance to identify the key responsibilities of federal CISOs established by federal law and guidance. We also evaluated information security policies and procedures from each of the 24 departments and agencies covered by the Chief Financial Officers Act<sup>10</sup> to determine if CISOs had been assigned a role in ensuring that information security activities were implemented in accordance with relevant laws and guidance.

Additionally, we administered a web-based survey to the CISOs of the 24 departments and agencies. In the survey, we asked the CISOs to identify (1) whether they felt that they had sufficient levels of responsibility and authority, and (2) challenges they faced in exercising their authority. We then interviewed each of the CISOs who were in place at the time of our review in order to validate responses from the survey and to obtain additional insight into the challenges they identified. In addition, we met with representatives from OMB to discuss OMB's role in providing guidance to clarify the responsibilities and authorities of federal CISOs.

We conducted this performance audit from June 2015 to August 2016 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

---

<sup>10</sup>The 24 Chief Financial Officers Act agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development (31 U.S.C. § 901(b)).

---

the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A more complete description of our objectives, scope, and methodology is provided in appendix I.

---

## Background

Safeguarding federal computer systems and the systems supporting the nation's critical infrastructures is essential to protecting national and economic security, and public health and safety. For government organizations, information security is also a key element in maintaining the public trust. Inadequately protected systems may be vulnerable to insider threats as well as the risk of intrusion by individuals or groups with malicious intent who could use their illegitimate access to obtain sensitive information, disrupt operations, or launch attacks against other computer systems and networks. Our previous reports,<sup>11</sup> and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, and inappropriate disclosure.

The emergence of increasingly sophisticated cyber threats underscores the need to manage and bolster the security of federal information systems. For example, advanced persistent threats—where an adversary that possesses sophisticated levels of expertise and significant resources can attack using multiple means such as cyber, physical, or deception to achieve its objectives—pose increasing risks. In addition, the number and types of cyber threats are on the rise. The attack on federal personnel and background investigation files that breached the PII of more than 20 million federal employees and contractors illustrates the need for strong security over information and systems. Further, in February 2015, the Director of National Intelligence testified<sup>12</sup> that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.

---

<sup>11</sup>See, for example, GAO, *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, [GAO-15-714](#) (Washington, D.C.: Sept. 29, 2015).

<sup>12</sup>Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, testimony delivered on February 26, 2015.

---

## Federal Law and Guidance Establish Information Security Requirements

FISMA establishes information security program and evaluation requirements for federal agencies in the executive branch. To help protect against threats to federal systems, FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support its operations and assets, including those provided or managed by another agency, contractor, or another organization on its behalf. FISMA also states that the agency head is to delegate authority to ensure compliance with the law to the CIO, who in turn is to designate a senior agency information security officer to carry out the CIO's responsibilities under the law. In most federal organizations, this official is referred to as the CISO.

FISMA also assigns responsibilities to OMB, the Department of Homeland Security (DHS), NIST, and agency inspectors general:

- OMB's responsibilities include, among other things, developing and overseeing the implementation of policies, principles, standards, and guidelines on information security in federal agencies except with regard to national security systems.<sup>13</sup> Since 2003, OMB has issued requirements and guidance to agencies on many information security issues, such as an initiative to consolidate and secure agencies' connections to the Internet; the security of cloud computing; privacy and the protection of PII; and continuous monitoring of security controls in federal information systems. Additionally, OMB has issued annual instructions for agencies and inspectors general to meet requirements for reporting on the effectiveness of agency security programs.
- DHS's responsibilities under FISMA 2014 include, among other things, developing, issuing, and overseeing implementation of binding operational directives to agencies, including directives for incident reporting, contents of annual agency reports, and other operational requirements. DHS issued the first binding operational directive under

---

<sup>13</sup>As defined in FISMA, the term "national security system" means any information system used by or on behalf of a federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications) or (2) is protected at all times by procedures established for handling classified national security information. 44 U.S.C. § 3552(b)(6)(A).

---

its FISMA 2014 authorities in May 2015, mandating that federal agencies mitigate all critical vulnerabilities in Internet-accessible systems within 30 days.<sup>14</sup>

- NIST's chief responsibility under FISMA is to develop security standards and guidelines for agencies.<sup>15</sup> In accordance with its statutory responsibilities, NIST has developed a risk management framework of standards and guidelines for agencies to follow in developing and implementing information security programs.
- Each agency inspector general, or other independent auditor, is required to annually evaluate and report on the information security program and practices of the agency. In September 2015, we reported that, according to agency inspectors general, the extent of agencies' implementation of requirements for establishing and maintaining an information security program was mixed.<sup>16</sup> We noted that our work and reviews by inspectors general had highlighted information security control deficiencies at agencies that exposed information and information systems supporting federal operations and assets to elevated risk of unauthorized use, disclosure, modification, and disruption.

Additionally, OMB Circular A-130<sup>17</sup> requires that agency information security and privacy programs provide for agency information security and privacy policies, planning, budgeting, management, implementation, and oversight; and cost-effectively manage information security and privacy risks, including reducing such risks to an acceptable level. It also requires agencies to implement a risk management framework to guide and inform (1) the categorization of federal information and information systems, (2) the selection, implementation, and assessment of security and privacy controls, (3) the authorization of information systems and common controls, and (4) the continuous monitoring of information

---

<sup>14</sup>DHS Binding Operational Directive 15-01 "Critical Vulnerability Mitigation Requirement for Federal Civilian Branch Departments and Agencies' Internet-Accessible Systems" (May 21, 2015).

<sup>15</sup>NIST's responsibilities for security standards and guidelines were prescribed by FISMA 2002 and continue unchanged by FISMA 2014.

<sup>16</sup>[GAO-15-714](#).

<sup>17</sup>OMB, Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

---

systems. Additionally, the circular requires agencies to ensure that the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with FISMA 2014.

---

## Most Federal Agencies Defined the Role of the CISO in Accordance with Federal Law and Guidance

FISMA states that each agency head is responsible for securing agency information and information systems, including by delegating to the agency CIO the authority to ensure compliance with the law's requirements. The CIO, in turn, is directed to designate a CISO to carry out the CIO's responsibilities. Those responsibilities include ensuring the development, documentation, and implementation of the agency-wide information security program. We found that most agencies had defined the role of the CISO in ensuring that most security program activities were developed, documented, or implemented in their policies. However, 14 agencies had not defined the CISO's role for all required activities, potentially limiting these officials' ability to effectively oversee these agencies' information security programs. In particular, for several components of their information security programs, these agencies either assigned these responsibilities to other officials within the agency or did not document the role their CISO played. Without fully defining this role for all of the elements of their information security programs, agencies are not positioning their CISOs to most effectively carry out their responsibilities for ensuring compliance with federal information security requirements and effectively manage risks to their operations.

---

## Federal Law and Guidance Establish Responsibilities of CISOs

Under FISMA, the agency CISO is to carry out the CIO's responsibilities for ensuring agency compliance with the law, including development, documentation, and implementation of the agency-wide information security program that includes the following eight components:

- **Periodic risk assessments:** FISMA requires agencies to conduct 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. These risk assessments help determine whether controls are in place to remediate or mitigate risk to the agency. According to NIST guidance, risks are addressed from an organizational perspective with the development of, among other things, risk management policies, procedures, and strategy. The risk decisions made at the organizational level are to guide the entire risk management program. At the information system level, risk management activities include

---

categorizing organizational information systems, allocating security controls to organizational information systems, and managing the selection, implementation, assessment, authorization, and ongoing monitoring of security controls.<sup>18</sup>

- **Policies and procedures:** Agencies are required to develop, document, and implement 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.
- **Security plans:** Information security programs are required 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 a 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. In addition, NIST recommends that the plan be reviewed and updated at least annually.<sup>19</sup>
- **Security awareness 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.
- **Periodic testing:** Federal agencies are required to 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 information

---

<sup>18</sup>NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Special Publication (SP) 800-37 Revision 1 (Gaithersburg, Md.: February 2010).

<sup>19</sup>NIST, *Guide for Developing Security Plans for Federal Information Systems*, SP 800-18 Revision 1 (Gaithersburg, Md.: February 2006).

---

systems. This type of oversight is a fundamental element that demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results are used to improve security.

- **Remedial actions:** FISMA requires agencies to plan, implement, evaluate, and document remedial actions to address any deficiencies in their information security policies, procedures, and practices. In addition, NIST guidance states that federal agencies should develop a plan of action and milestones (POA&M) for information systems to document the agency'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.<sup>20</sup> Furthermore, the POA&M should identify, among other things, the resources required to accomplish the tasks and scheduled completion dates for the milestones. 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.
- **Incident response:** FISMA requires that agency security programs include procedures for detecting, reporting, and responding to security incidents and that agencies report incidents to the United States Computer Emergency Readiness Team. According to NIST, incident response capabilities are necessary for rapidly detecting an incident, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.<sup>21</sup>
- **Contingency planning:** FISMA requires federal agencies to implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. According to NIST, contingency planning is part of overall information system continuity of operations planning, which fits into a

---

<sup>20</sup>NIST, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Special Publication (SP) 800-53A, Revision 4 (Gaithersburg, Md.: December 2014).

<sup>21</sup>NIST, *Computer Security Incident Handling Guide*, SP 800-61 Revision 2 (Gaithersburg, Md.: August 2012).

---

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 (IT) and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, and testing it and making the necessary adjustments.<sup>22</sup>

Other important requirements of FISMA that are required to be carried out by the CISO include the following:

- **Specialized security training:** Agencies are required to train and oversee personnel who have significant information security responsibilities. According to NIST, a needs assessment is crucial to identify the individuals with significant IT security responsibilities, assess their functions, and identify their training needs. Training material should be developed that provides the skill sets necessary for attendees to accomplish the security responsibilities associated with their jobs. Examples of positions that would typically require specialized training include system administrators, system owners, security program managers, and senior agency leaders.<sup>23</sup>
- **Contractor system security oversight:** Under FISMA, agency information security programs are to provide security for the information and systems supporting the operations and assets of the agency, including systems provided or managed by contractors. In addition, OMB's annual FISMA reporting instructions require agencies to develop policies and procedures for agency officials to follow when performing oversight of the implementation of security and privacy controls by contractors.

---

<sup>22</sup>NIST, *Contingency Planning Guide for Federal Information Systems*, NIST SP 800-34 Revision 1 (Gaithersburg, Md.: May 2010).

<sup>23</sup>NIST, *Building an Information Technology Security Awareness and Training Program*, SP 800-50 (Gaithersburg, Md.: October 2003).



---

Additionally, OMB requirements and NIST guidance<sup>24</sup> call for agencies, as part of the information security program, to authorize the operation of information systems and explicitly accept any associated risks to organizational operations and assets, individuals, other organizations, and the nation, based on the implementation of an agreed-on set of security controls. According to NIST, the system security plan, the results of the security control assessment, and POA&Ms describing planned remedial actions provide the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

---

### Most Agencies Defined the Role of the CISO for Most Information Security Program Activities

For the 11 activities that we evaluated, 11 of the 24 agencies had fully defined the role of the CISO for all 11 activities. The other 13 agencies varied in their definitions of the CISO's role, from defining the role for most activities (11 agencies) to a few activities (2 agencies). Table 1 outlines the extent to which each of the 24 federal agencies defined the role of the CISO in their information security policies in accordance with FISMA and other federal requirements and guidance.

---

<sup>24</sup>NIST 800-37.

**Table 1: Extent to Which 24 Agencies Defined the Role of Their Chief Information Security Officer**

	Periodic risk assessments	Policies and procedures	Security plans	Security awareness training	Periodic testing	Remedial actions	Incident response	Contingency planning	Specialized security training	Contractor systems	System authorization
Department of Agriculture	●	●	●	●	●	●	●	●	●	●	●
Department of Commerce	●	●	●	●	●	●	●	○	●	●	●
Department of Defense	●	○	●	●	●	●	○	●	●	○	●
Department of Education	●	●	●	●	●	●	●	●	●	●	●
Department of Energy	●	●	○	○	●	○	●	○	●	○	○
Department of Health and Human Services	●	●	●	●	●	●	●	○	●	●	●
Department of Homeland Security	●	●	●	●	●	●	●	●	●	●	●
Department of Housing and Urban Development	●	●	●	●	●	●	●	●	●	●	●
Department of the Interior	●	●	○	●	●	●	●	○	●	○	○
Department of Justice	●	○	●	●	●	●	●	○	●	●	●
Department of Labor	●	●	●	●	●	●	●	●	●	●	●
Department of State	●	●	●	●	●	●	○	●	●	●	●
Department of Transportation	●	●	○	●	○	●	●	●	●	●	●
Department of the Treasury	●	●	○	○	○	●	●	○	○	○	○
Department of Veterans Affairs	●	●	●	●	●	●	●	●	●	●	●
Environmental Protection Agency	●	●	○	●	●	●	●	○	●	●	○
General Services Administration	●	●	●	●	●	●	●	●	●	●	●
National Aeronautics and Space Administration	●	●	●	●	●	●	●	●	●	○	●
National Science Foundation	●	●	●	●	●	●	●	●	●	●	●
Nuclear Regulatory Commission	●	●	●	●	●	●	●	●	●	●	●
Office of Personnel Management	●	●	●	●	●	●	●	●	●	●	●
Small Business Administration	●	●	●	●	●	●	●	●	○	●	●
Social Security Administration	●	●	●	●	●	●	●	●	●	●	●
U.S. Agency for International Development	●	●	●	●	●	●	●	●	●	○	●

Legend:

- Role for CISO defined in agency policy.
- No role for CISO defined in agency policy.

Source: GAO analysis of agency information security policies. | GAO-16-686

---

All Agencies Defined CISO Responsibilities for Periodic Risk Assessments

Each of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that risk to the agency's information and information systems was assessed periodically. For example:

- The Department of Commerce (Commerce) assigned responsibility for developing and implementing a department-wide risk management strategy and implementing a cyber security risk management framework to the Office of Cyber Security, which is headed by the CISO.
- The Department of Veterans Affairs' (VA) risk management policy stated that the CISO is responsible for working with other VA IT organizations to establish risk action plans, working with stakeholders on implementing those plans, and evaluating and monitoring the internal risk environment.
- The Social Security Administration (SSA) delegated responsibility for risk management to the Office of Information Security, which is headed by the SSA CISO.

By defining the CISO's role in periodic risk assessments, agencies will have greater assurance that the CISO is aware of the risks to essential computing resources and can make informed decisions about needed security protections.

Nearly All Agencies Defined the CISO's Responsibilities for Information Security Policies and Procedures

Twenty-two of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that risk-based information security policies and procedures were established. For example:

- The U.S. Department of Agriculture (USDA) information security program assigned responsibility for formulating and issuing departmental cyber security policies and procedures to the CISO.
- The Department of Transportation (DOT) CISO was responsible for providing management leadership in cybersecurity policy and guidance. Additionally, the CISO was responsible for reviewing and approving cybersecurity policies and procedures developed by departmental components.
- The General Services Administration assigned the CISO responsibility for annually reviewing and revising the agency's information security policy, and for developing and publishing IT security procedural guides.

---

However, two agencies—the Departments of Defense and Justice—did not define the CISO’s responsibilities for this activity in their policies:

- The Department of Defense (DOD) senior information security officer (SISO)<sup>25</sup> told us that the responsibilities of the SISO organization included developing and maintaining policies and procedures; however, these responsibilities were not documented in DOD policy.
- The Department of Justice (DOJ) CISO indicated that the information security office was responsible for security policies and procedures; however, this was not described in the department’s information technology security policy.

By ensuring that the CISO’s role is defined for establishing policies and procedures, these two agencies will have increased assurance that CISOs are able to effectively reduce risks to their information and information systems, and that the information security practices that are driven by these policies and procedures are consistently applied.

Agencies Did Not Always Define the CISO’s Responsibilities for Security Plans

Nineteen of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that plans for providing security for information systems were in place. For example:

- The Department of Education security policy assigned the CISO responsibility for ensuring that security authorization documents, including system security plans, are complete, consistent, and in compliance with security standards.
- The Department of Labor’s security policy stated that the information security team, which is headed by the CISO, reviews the system security plan for each information system as part of its authorization oversight responsibilities.
- The Small Business Administration assigned the CISO responsibility for reviewing system security plans and other system documentation to ensure that security requirements have been adequately addressed.

---

<sup>25</sup>The Department of Defense refers to the department-level CISO position as the senior information security officer.

---

However, five agencies—the Departments of Energy, the Interior, Transportation, and the Treasury; and the Environmental Protection Agency—did not define developing, reviewing, or updating system security plans as a CISO responsibility in their policies:

- Although the Department of Energy (DOE) delegated the authority to carry out the responsibilities of the CIO under FISMA, including developing and maintaining the DOE-wide information security program, to the DOE CISO, the department’s cybersecurity program order did not document any responsibilities for the CISO in overseeing system security plans.
- In a written response, officials from the Department of the Interior (Interior) stated that CISO staff oversees security plans through the department’s central FISMA compliance repository. However, although Interior’s assessment and authorization package documentation policy stated that system authorization documentation is to be maintained in the repository, it did not document the CISO office’s responsibilities for oversight of this documentation, including security plans.
- DOT officials stated in a written response that the CISO’s office reviews a sample of system security plans and documentation annually, based on prior year audit findings or systems of significant criticality or impact. However, although DOT’s guide for security authorization and continuous monitoring stated that the CISO conducts oversight reviews of component cybersecurity programs, it did not indicate that security plans were included in these reviews.
- In a written response, officials from the Department of the Treasury (Treasury) stated that, although the department’s policy required FISMA reporting and other cybersecurity information, including security plans, to be reported to the CIO, the CISO organization actually collects, oversees, and manages this process. However, these responsibilities were not specified in policy.
- The Environmental Protection Agency (EPA) senior agency information security officer (SAISO)<sup>26</sup> stated that the agency was working to implement a new process in which system authorization

---

<sup>26</sup>The Environmental Protection Agency refers to the agency-level CISO position as the senior agency information security officer.

---

packages—which include security plans—would be routed through the SAISO organization for review. He indicated that the process was expected to be implemented in the summer of 2016.

Until these five agencies appropriately define the role of the CISO in ensuring that system security plans are appropriately documented, these CISOs may be unable to effectively ensure that their agency's officials are aware of system security requirements or whether controls are in place.

#### Nearly All Agencies Defined the CISO's Responsibilities for Security Awareness Training

Twenty-two of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that all employees received information security training. For example:

- Commerce assigned the Office of Cyber Security, headed by the CISO, the responsibility to maintain the department's information security awareness and training program, including establishing requirements for training for operating units and monitoring compliance.
- DHS's information security policy directive stated that the CISO is responsible for ensuring that department personnel, contractors, and others working on behalf of DHS receive information security awareness training.
- SSA assigned the CISO the responsibility to develop SSA's security awareness training policy, provide information on training opportunities that meet the requirements of the policy, and oversee the implementation of the training program.

However, two agencies—the Departments of Energy and the Treasury—did not define the CISO's responsibilities for security awareness training in their policies:

- Although DOE delegated the authority to carry out the responsibilities of the CIO under FISMA, including developing and maintaining the DOE-wide information security program, to the DOE CISO, the department's Cybersecurity Awareness and Training Program policy did not define the roles and responsibilities of the CISO with respect to security awareness training.
- In a written response, Treasury officials stated that the department CISO collects and manages department-wide data on training completion. However, although Treasury policy states that bureaus are to provide materials and assistance to support the oversight and

---

---

Most Agencies Defined the CISO's Roles in Oversight of Security Control Testing Activities

central reporting roles of the Treasury Cybersecurity Office, it did not specify that training completion data are to be provided. Additionally, officials stated that the CISO provides a web-based security awareness training tool for bureaus, but this was not documented in Treasury's security policies.

By defining the CISO's role in ensuring that all users receive security awareness training, DOE and Treasury can better equip their CISOs to ensure that their agency personnel have a basic understanding of information security requirements to protect the systems they use.

Twenty-two of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that security controls are tested periodically in accordance with FISMA and NIST guidance. For example:

- VA assigned the CISO responsibility for establishing and monitoring the department's Information Security Continuous Monitoring program, including ensuring that reports are monitored and that issues identified are escalated for appropriate action.
- DHS's security policy stated that the CISO is responsible for ensuring that organizational security testing plans are executed in a timely manner.
- The Office of Personnel Management's (OPM) security policy and guidance indicated that the CISO is responsible for reviewing the results of periodic testing as part of the oversight of system authorization activities.

However, two agencies—the Departments of Transportation and the Treasury—did not define the CISO's responsibilities for ensuring that security controls are tested periodically across the agency in their policies:

- DOT officials stated in a written response that the CISO office annually tests a sample of security controls as part of its compliance activities. However, although DOT's guide for security authorization and continuous monitoring stated that the CISO conducts oversight reviews of component cybersecurity programs, it did not indicate that the reviews included any oversight of security testing.
- Treasury officials stated in a written response that responsibility for security testing had been delegated to bureaus. They also stated that the security policy describes oversight of security testing by the CISO;

---

---

Nearly All Agency Policies Defined CISO Responsibilities for Oversight of Remedial Actions

however, although the policy stated that security controls are to be tested on an ongoing basis as part of a continuous monitoring process, it did not describe any responsibilities for the CISO or the CISO office for ensuring that security controls are periodically tested.

If these two federal agencies define the CISOs role in ensuring that security controls are periodically tested, these officials will be better able to ensure that security controls have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency.

Twenty-three of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that remedial actions are documented and used to address identified deficiencies in security controls. For example:

- The Department of Housing and Urban Development assigned the Office of Information Technology Security, which is headed by the CISO, the responsibility for ensuring that POA&Ms for the security program and information systems are maintained and documented.
- Treasury's information security policy stated that the CISO is responsible for monitoring information system weaknesses at the bureaus and implementation of corrective actions.
- Interior assigned responsibility for reviewing bureau- and office-level POA&Ms and ensuring that they comply with department-wide and OMB guidance to the CISO. Additionally, the CISO is responsible for ensuring that all bureau and office information systems' weaknesses are adequately described and that planned corrective actions appropriately address the weaknesses.

However, DOE did not identify who was responsible for ensuring that remedial actions are taken and are effective in its policies. Specifically, DOE delegated the authority to carry out the responsibilities of the CIO under FISMA, including developing and maintaining the DOE-wide information security program, to the DOE CISO. However, the department's cybersecurity program order did not specify any responsibilities for the CISO in overseeing remedial actions. The DOE CISO stated that overall responsibility for the remedial action process is assigned to the CIO, and that the CIO reviews POA&M reports for significant weaknesses. He also stated that the CISO uses POA&Ms to understand the environment of a particular site prior to going on a site visit. However, these responsibilities were not documented in DOE's



---

---

Agencies Almost Always Defined the CISO's Responsibilities for Incident Detection, Response, and Reporting in Policy

cyber security program policy. By defining the CISO's role in ensuring that the agency has remediation processes, DOE will have greater assurance that their CISOs are able to ensure that control weaknesses affecting the agency's information and information systems are being corrected and addressed in a timely manner.

Twenty-two of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that the agency has procedures for detecting, reporting, and responding to security incidents. For example:

- Interior assigned responsibility for this activity to its Computer Incident Response Center, which is part of the Information Assurance Division led by the CISO.
- The U.S. Agency for International Development's (USAID) security policies stated that the CISO is to establish and update incident response policies and procedures, and that the CISO is the central authority for coordinating and reporting sensitive and national security incidents for the agency.
- The National Science Foundation assigned the CISO responsibility for overseeing the Computer Incident Response Team during responses to reported incidents.

However, two agencies—the Departments of Defense and State—did not define the CISO's responsibilities for this activity in their policies:

- DOD assigned responsibility for incident response to Cyber Command, within U.S. Strategic Command. The DOD SISO told us that the SISO organization is involved in Cyber Command's incident response activities; however, these responsibilities and activities were not documented in the department's security policies.
- The Department of State (State) assigned responsibility for incident response to the Office of Cybersecurity in the Bureau of Diplomatic Security. The State CISO and the Director of the Office of Cybersecurity stated that the department has deliberately assigned certain operational cybersecurity functions and program responsibilities to the Bureau of Diplomatic Security.

By defining the role of the CISO in ensuring that the agency has procedures for incident detection, reporting, and response, DOD and State will help their CISOs ensure that the agency's information and information systems are adequately protected from cyber attacks.

---

CISO Responsibilities for  
Contingency Planning Were  
Not Always Defined

Seventeen of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that plans and procedures are in place to ensure recovery and continued operations of their information systems in the event of a disruption. For example:

- VA's information security program policy stated that the CISO is responsible for working closely with IT and other business units to develop and maintain an enterprise business continuity program; managing the planning, design, maintenance of business continuity program projects and ensuring compliance with industry standards and regulatory requirements; monitoring the development of business continuity plans and reviewing plans to ensure compliance; and providing business and technical guidance relative to business continuity.
- DHS assigned the CISO responsibility for reviewing and approving contingency plans, and for ensuring that plans for ensuring the continuity of operations for information systems are developed and maintained.
- OPM's security policy stated that the CISO reviews system contingency plans and requires that the results of contingency plan tests and exercises be provided to the CISO.

However, seven agencies—the Departments of Commerce, Energy, Health and Human Services, the Interior, Justice, and the Treasury; and the Environmental Protection Agency—did not define the CISO's responsibilities for contingency planning in their policies:

- Commerce assigned this responsibility to the Critical Infrastructure Protection Manager, and did not describe any role for the CISO in the department's information technology security program policy.
- Although DOE delegated the authority to carry out the responsibilities of the CIO under FISMA, including developing and maintaining the DOE-wide information security program, to the DOE CISO, the department's continuity program order did not describe any responsibilities for the CISO.
- The Department of Health and Human Services' policy assigned responsibility for updating and maintaining the information technology contingency plan to a Contingency Planning Coordinator; the policy did not describe the oversight responsibilities of the CISO.

- 
- Interior officials stated in a written response that the CISO office funds a yearly audit which evaluates the implementation of security program activities, including continuity of operations activities, across the department; they also stated that the CISO office works with the Department's Office of Emergency Management to ensure integration of IT system contingency plans with the larger departmental continuity of operations plans. However, these activities were not defined in Interior's policies.
  - The DOJ CISO stated that her office regularly reviews system contingency plans and test results. However, this responsibility was not documented in DOJ's security policies.
  - Treasury officials provided documentation showing that the CISO office tracks contingency plan testing activities as part of its oversight activities. However, these responsibilities were not described in policy.
  - EPA's SAISO told us that the agency plans to implement a procedure for reviewing authorization packages, including contingency plans; he indicated that the process was expected to be implemented in the summer of 2016.

By not defining the CISO's role in contingency planning, these seven agencies may hinder their CISOs' ability to effectively ensure that information system contingency planning plans and procedures are in place, reducing the likelihood that these agencies will be able to successfully recover their systems in a timely manner in the event of a service disruption.

#### Nearly All Agencies Defined the CISO's Responsibilities for Specialized Security Training

Twenty-two of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that personnel with significant information security responsibilities were trained. For example:

- EPA assigned its SAISO the responsibility to develop and maintain role-based training, education, and credentialing requirements for personnel with significant information security responsibilities.
- USAID's security policy stated that the CISO is responsible for establishing and managing an information security training program, including training for personnel with significant security responsibilities and maintaining training records.
- The General Services Administration assigned the CISO responsibility for ensuring that Information Systems Security Officers and

---

Information Systems Security Managers receive applicable training specific to their information security responsibilities.

However, two agencies—the Department of the Treasury and the Small Business Administration—did not define the CISO’s responsibilities for this activity in their policies:

- In a written response, Treasury officials stated that the department CISO collects and manages department-wide data on training completion. However, although Treasury policy states that bureaus are to provide materials and assistance to support the oversight and central reporting roles of the Treasury Cybersecurity Office, it did not specify that training completion data are to be provided.
- The Small Business Administration CIO told us that the CISO is responsible for overseeing role-based security training across the agency; however, this responsibility was not reflected in the agency’s security policies.

Unless these two agencies define the roles of their CISOs in ensuring that personnel with significant security responsibilities receive appropriate training, their CISOs may be unable to ensure that these individuals have the 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.

Agency Policies Did Not Always Describe CISO Responsibilities for Oversight of Contractor System Security

Eighteen of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that contractor systems adhere to agency and federal information security requirements. For example:

- Thirteen agencies’ policies indicated that the CISO exercises oversight of contractor system security as part of the CISO’s overall oversight of the system authorization process.
- OPM’s security policy stated that the CISO is to conduct and coordinate information security audits at OPM and contractor facilities, and that the CISO organization reviews security clauses in contracts and statements of work.
- USDA assigned the CISO responsibility for conducting reviews of system documentation, including the system security plan, security assessment report, and plans of action and milestones, for all systems including contractor systems.

---

However, six agencies—the Departments of Defense, Energy, the Interior, and the Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development—did not define the CISO’s responsibilities in ensuring that contractor systems met security requirements in their policies:

- DOD policies did not describe the responsibilities of the SISO in ensuring that contractor systems met security requirements. The DOD SISO told us that the information security oversight organization was not currently conducting inspections of unclassified contractor networks. He also stated that the SISO office monitors self-reported data from contractors; however, these responsibilities were not defined in DOD’s policies.
- The DOE CISO stated that the CISO exercises some oversight of contractor system security through FISMA reporting responsibilities. However, although DOE delegated the authority to carry out the responsibilities of the CIO under FISMA, including developing and maintaining the DOE-wide information security program, to the DOE CISO, the department did not define the CISO’s responsibilities for oversight of contractor system security in its policies.
- In a written response, Interior officials stated that contractor systems are included in the authorization process, and that the CISO office oversees the authorization activities through yearly program audits and the audit activities of the Compliance and Audit Management Branch. However, these activities were not defined in Interior’s policies.
- Treasury’s information technology security program specified that it applied to contractor systems and department-owned systems; however, it did not define the CISO’s role in ensuring that contractor systems met security requirements.
- At the National Aeronautics and Space Administration, the SAISO<sup>27</sup> issued the agency’s policy for conducting security assessments of third-party information systems. However, the policy did not define the SAISO’s responsibilities for oversight of contractor security.

---

<sup>27</sup>The National Aeronautics and Space Administration refers to the agency-level CISO position as the SAISO.

- 
- USAID’s policy stated that responsibility for oversight of contractor system security was assigned to the contracting officer’s representative; the policy did not describe any role for the CISO or CISO office in this process. The USAID CISO agreed, and stated that the CISO had no way to verify that contractors were meeting security requirements.

Because these six agencies have not defined their CISOs’ responsibilities for oversight of contractor systems security, increased risk exists that weaknesses in these agencies’ contractor-operated systems may go undetected and unresolved.

#### Most Agencies Defined the CISO’s Responsibilities for Oversight of the System Authorization Process

Twenty of the 24 agencies defined the responsibilities of the CISO or CISO office in ensuring that information systems are authorized to operate in accordance with federal requirements. For example:

- The Department of Labor’s information security organization, headed by the CISO, administers the security authorization oversight process, which includes security plan reviews and verification of a sample of security controls.
- The Department of State’s information security policies state that the Information Assurance office, which is headed by the CISO, is responsible for ensuring that all departmental information systems go through the approved system authorization process.
- The Nuclear Regulatory Commission assigned the CISO responsibility for ensuring that information security risks are managed consistently throughout the agency by being incorporated into the system authorization process.

However, four agencies—the Departments of Energy, the Interior, and the Treasury; and the Environmental Protection Agency—did not define the CISO’s role in ensuring that systems were authorized in their policies:

- Although DOE delegated the authority to carry out the responsibilities of the CIO under FISMA, including developing and maintaining the DOE-wide information security program, to the DOE CISO, the department’s cybersecurity program order did not describe any specific roles or responsibilities for the CISO in ensuring that information systems are authorized to operate.
- Interior officials stated in a written response that the CISO office oversees authorization activities through yearly program audits and

---

the audit activities of the Compliance and Audit Management branch. However, these activities were not defined in Interior's policies.

- Treasury's information security policy indicated that the CISO is responsible for implementing the IT security program and performing compliance oversight, but did not describe any oversight responsibilities for the system authorization process beyond this general statement. In a written response, officials stated that, although the department's policy required FISMA reporting and other cybersecurity information to be reported to the CIO, the CISO organization actually collects, oversees, and manages this process; they also stated that the CISO office tracks the status of security authorization activities as part of its oversight activities. However, these responsibilities were not specified in policy.
- EPA's information security policy stated that the SAISO is to develop, implement, and maintain security authorization and reporting capabilities; however, it did not describe any role for the SAISO in the authorization process. The agency planned to update its processes to ensure that authorization packages were vetted through the SAISO's office. The EPA SAISO indicated that the process was expected to be implemented in the summer of 2016.

Unless CISOs at these four agencies have a clear role in system authorization decisions, the agencies will face greater difficulty ensuring that such decisions appropriately consider information security risks.

---

## Federal CISOs Identified Challenges to Their Authority That Limit Their Ability to Effectively Manage Agency-Wide Information Security Programs

Agency CISOs identified a number of challenges to their authority.<sup>28</sup> Specifically, in our survey of 24 agency-level CISOs, the following factors were frequently cited as presenting challenges to CISOs' ability to effectively carry out their responsibilities to ensure that information security program activities are implemented: (1) competing priorities between agency operations and information security, (2) coordination with component organizations and other offices, (3) availability of security-related information from component organizations and IT contractors, (4) oversight of indirect reports and IT contractors, and (5) the position of the CISO in the agency's hierarchy. Respondents also reported challenges related to other factors that did not directly affect their authority but nevertheless may limit their ability to carry out their responsibilities.

There are several government-wide initiatives under way that are intended to help address some of these challenges. However, although OMB has responsibility under FISMA for providing guidance to federal agencies,<sup>29</sup> it has not issued guidance clarifying how agencies should implement recent provisions in federal law aimed at strengthening their oversight of information security activities<sup>30</sup> or the role of agency CISOs in carrying them out. This lack of clarity further hinders CISOs' ability to address challenges to their authority, including balancing operational and security needs, overseeing security activities, obtaining adequate and timely information, and ensuring that senior managers are aware of information security risks facing the agency.

---

## Many CISOs Reported Challenges to Their Authority

### Competing Priorities between Operations and Security

Eighteen CISOs reported that competing priorities between agency operations and information security challenged their ability to exercise their responsibilities to ensure the implementation of the agency-wide information security program to a large or moderate extent, as shown in figure 1 below.

---

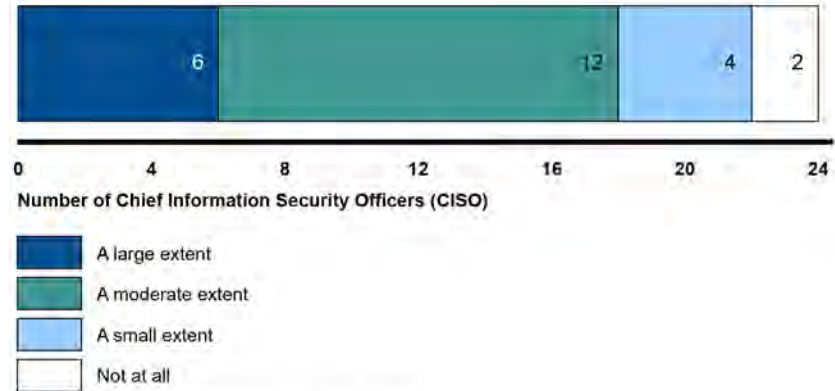
<sup>28</sup>For purposes of our survey of agency CISOs, we defined "authority" as the power to control and influence the outcome of activities within the CISO's scope of responsibility.

<sup>29</sup>44 U.S.C. 3553(a).

<sup>30</sup>44 U.S.C. § 3554(a)(6) & (7).



**Figure 1: Extent to Which 24 Agency Chief Information Security Officers Identified Competing Priorities between Agency Operations and Information Security as Challenging**



Source: CISO responses to GAO survey | GAO-16-686

Respondents identified several specific challenges related to this factor. For example, one respondent stated that security personnel at the component level report to the component’s management chain rather than to the CISO; consequently, they are often driven by the operational imperatives of the component agency rather than the security priorities of the department. The respondent also noted that programs often view cybersecurity as a drain on limited resources. Another CISO explained that agency operations drive procurements at a faster pace than is feasible for their cyber team to track. Another CISO expressed a similar sentiment, stating that technology is advancing rapidly and security is often seen as getting in the way of progress. Another respondent noted that the operational priorities of the agency tend to favor maintaining existing operations rather than correcting weaknesses and vulnerabilities in a timely fashion.

According to NIST SP 800-39,<sup>31</sup> effective risk management requires an organization’s mission/business processes to explicitly account for information security risk when making operational decisions. When organizations make operational decisions without adequately considering information security risk, CISOs are hindered in ensuring that appropriate

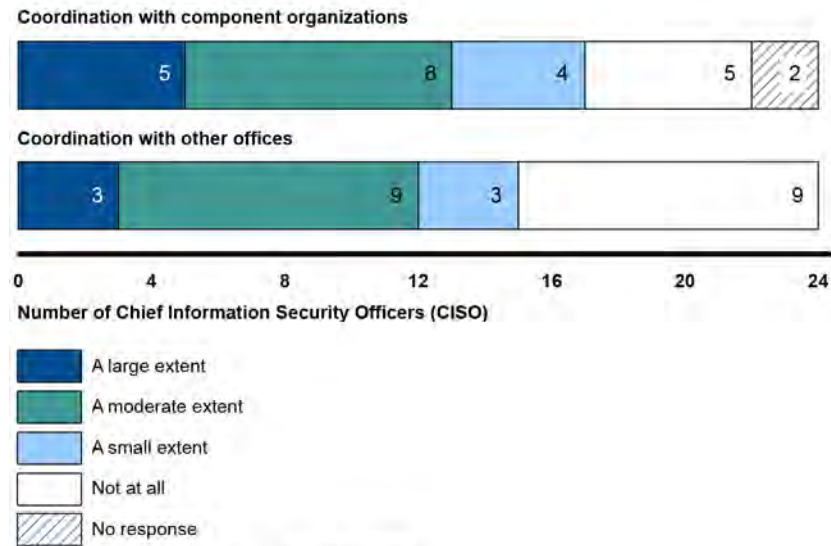
<sup>31</sup>NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

Coordination with Component Organizations and Other Offices

security controls are applied or that weaknesses are addressed prior to new systems or technology being deployed.

About half of the CISOs we surveyed reported challenges when coordinating with component organizations or with other offices (e.g., program, human capital, and contracting offices). Specifically, 13 reported that coordination with component organizations was challenging to a large or moderate extent, and 12 reported that coordination with other offices was challenging to a large or moderate extent, as shown in figure 2 below.

**Figure 2: Extent to Which 24 Agency Chief Information Security Officers Identified Coordination with Component Organizations and Other Offices as Challenging**



Source: CISO responses to GAO survey. | GAO-16-686

Respondents identified several specific challenges related to these factors. For example:

- Coordination with component organizations.* One CISO stated that risk decisions made by authorizing officials or system owners within components often exceeded the department’s standards for risk acceptance, because component organizations often had risk tolerances that were not consistent with the department’s. Another stated that coordinating with component organizations can slow incident response efforts, depending on the components’ resources, expertise, and priorities. Another respondent noted that the

---

department-level CISO lacks the authority to mandate that components implement decisions that have to be applied across the enterprise, although the CISO also noted that considerable support could be gained through using a collaborative approach. Another respondent indicated that system development life cycle management is not a mature process at many component organizations, and that some components do not apply a formal system development life cycle process.

- *Coordination with other offices.* One CISO noted that other offices that are responsible for enterprise controls have not always fully assumed the responsibility for overseeing, testing, and evaluating those controls. Another CISO stated that security controls that depend on other offices in the agency are not always recognized by those offices as priorities—or even as responsibilities—because the requirements do not arise from their own chain of authority. Another CISO stated that program offices at his agency frequently challenge the CISO’s authority to oversee contractors’ implementation of security controls in order to maintain the business relationship with the contractor. One respondent noted that, in system development efforts, security is seen by the project as a burden, making it difficult for the security organization to conduct oversight of the project life cycle.

NIST guidance states that organizations may choose to delegate authority, responsibility, and decision-making power for information security to individual subordinate organizations, such as bureaus or components within a federal agency, in order to accommodate subordinate organizations with divergent mission/business needs and operating environments.<sup>32</sup> However, if CISOs face difficulties coordinating with component organizations or other offices within their agencies, their ability to help ensure that information security risks are being identified and mitigated across the enterprise may be hindered.

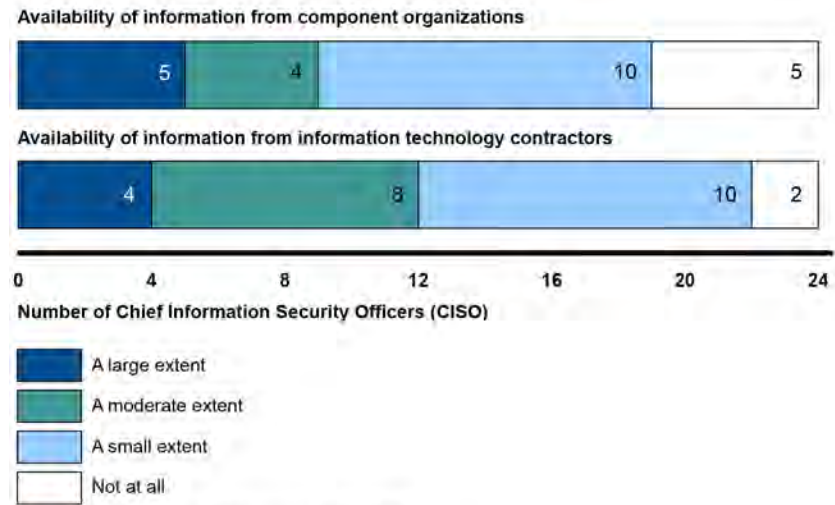
Limited Access to Information Security Data from Component Organizations and IT Contractors

Nine CISOs reported challenges to a moderate or large extent when receiving information security information from component organizations, and twelve reported that receiving information security information from IT contractors as challenges. Figure 3 below shows the extent to which CISOs identified these factors as challenging.

---

<sup>32</sup>NIST 800-39.

**Figure 3: Extent to Which 24 Agency Chief Information Security Officers Identified Availability of Security-Related Information from Component Organizations and IT Contractors as Challenging**



Source: CISO responses to GAO survey. | GAO-16-686

Respondents identified several specific challenges related to these factors. For example:

- Availability of information from components:* One respondent stated that a number of networks and systems are independently managed and maintained by components, which are frequently reluctant to share information with the department-level security organization. Another noted that the department-level security organization does not always have visibility into the networks or systems at component organizations. Another CISO stated that components do not always share complete information on security incidents with the central security organization, and that some do not involve the department-level security organization in incident investigations. The respondent further noted that system authorization data are self-reported by component organizations, making it difficult for the CISO organization to verify that the components are complying with departmental policy.
- Availability of information from IT contractors:* One respondent noted that contractual limitations can prevent access to information that would normally be available in a government-owned and -operated environment. Another stated that, even when language requiring contractors to provide the agency access to security information is included in contracts, it can still be very difficult to obtain necessary

---

information from contractors. One CISO noted that there are no means by which the agency can validate data reported by contractors.

According to NIST guidance for managing information security risk, it is important to ensure that risk-related information is shared among subordinate organizations and with the parent organization because the risk decisions by subordinate organizations may have an effect on the organization as a whole.<sup>33</sup> When CISOs have difficulty receiving adequate information security information from components or contractors, they may lack all of the information that they need to effectively carry out their responsibilities to oversee the security program activities for which those components or contractors are responsible.

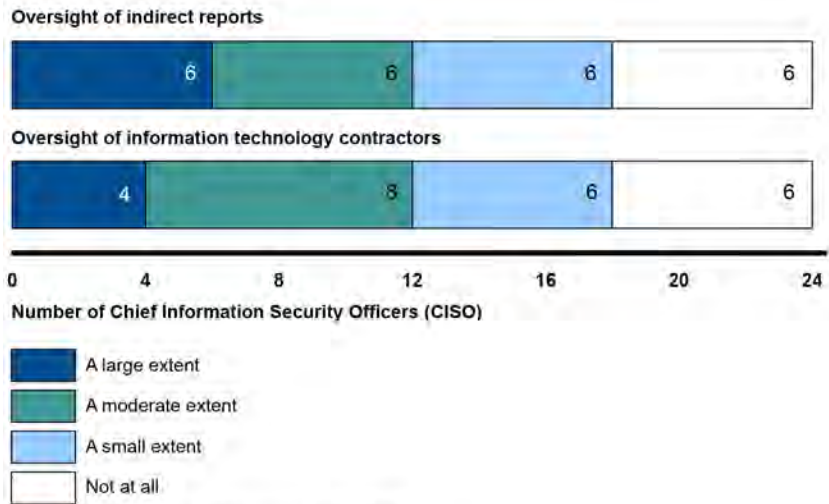
#### Oversight of Indirect Reports and IT Contractors

Half of CISOs reported that their ability to exercise oversight of individuals and offices outside of the CISO's direct reporting structure challenged them to a large or moderate extent. Additionally, half of the CISOs we surveyed also reported challenges related to oversight of IT contractors. Figure 4 below identifies the extent to which CISOs identified these factors as challenging.

---

<sup>33</sup>NIST 800-39.

**Figure 4: Extent to Which 24 Agency Chief Information Security Officers Identified Oversight of Indirect Reports and IT Contractors as Challenging**



Source: CISO responses to GAO survey. | GAO-16-686

Respondents identified several specific challenges related to these factors. For example:

- Oversight of indirect reports.* One respondent indicated that the CISO lacks the authority to hold indirect reports, such as information system security officers (ISSO),<sup>34</sup> accountable for carrying out their information security responsibilities. Another stated that the personnel supporting ongoing and deployed projects are not accountable to the CISO; rather, they are overseen by operations and engineering teams, whose priorities are focused on operations and delivering functionality and not on security.
- Oversight of IT contractors.* For example, one respondent stated that contractors not directly assigned to IT security reported to their

<sup>34</sup>According to NIST SP 800-37, the information system security officer is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system. The information system security officer also serves as a principal advisor on all matters involving the security of an information system. The information system security officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day security operations of a system.

---

sponsor program offices, and consequently oversight activities had to be coordinated through program managers, contracting officers, or their representatives. Another stated that the CISO did not have control over the cybersecurity contract that supports the information security organization. One CISO expressed difficulties in establishing a consistent interpretation of security requirements across component agencies' contracting organizations. Another also stated that the security organization lacks the authority to validate security documentation submitted by contractors.

NIST guidance states that leaders and managers at all levels of an organization need to understand their responsibilities and be held accountable for managing information security risk.<sup>35</sup> When CISOs experience difficulties overseeing the information security responsibilities of individuals outside of their reporting hierarchy or of IT contractors, they can be hindered in their ability to ensure that the actions of these individuals comply with the agency's security policies or sufficiently address the risks facing the agency.

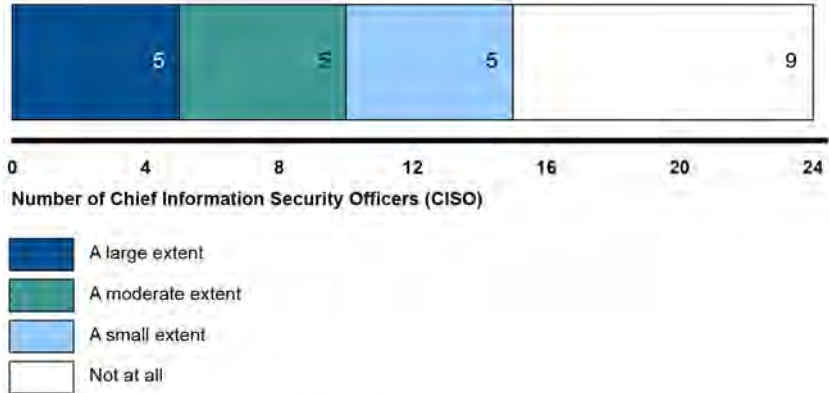
#### CISOs' Organizational Placement

Ten of the 24 CISOs reported that their position in the agency hierarchy challenged their ability to carry out their responsibilities to a large or moderate extent. Figure 5 below identifies the extent to which CISOs identified their position in the agency hierarchy as challenging.

---

<sup>35</sup>NIST 800-39.

**Figure 5: Extent to Which 24 Agency Chief Information Security Officers Identified Their Placement in the Agency Hierarchy as Challenging**



Source: CISO responses to GAO survey. | GAO-16-686

Respondents identified several specific challenges related to this factor. For example, one respondent noted that the department-level CISO resided under a department under secretary, which often blurred the lines of authority and accountability between the IT organization and other components. Another indicated that being positioned higher in the organization would make it easier to gain concurrence and support for security initiatives, and that the CISO's current position made it difficult to ensure that identified weaknesses are addressed and that incidents are being handled appropriately. Another respondent noted that the CISO's placement in the organization can limit their ability to elevate significant information security risks to upper management. However, one noted that an increased focus on cybersecurity issues at the agency in recent months has resulted in the CISO having greater access to agency leadership.

If CISOs are unable to hold component and office personnel accountable for taking action or elevate security concerns to upper management, they will be challenged in their ability to ensure that agency leaders have a clear understanding of the agency's risk profile, and agencies may be less able to effectively manage and respond to these risks.

### CISOs Reported That Other Factors Presented Challenges

The 24 CISOs also reported that other factors posed challenges to their ability to carry out their responsibilities effectively, including the following examples:



- 
- *Lack of sufficient staff.* CISOs identified challenges with having insufficient personnel to oversee security activities effectively. For example, one CISO noted that the information security office did not have enough personnel to oversee the implementation of the number and scope of requirements described in NIST SP 800-53 as well as to respond to FISMA audits and OMB data calls. Another noted that the agency's security operations center did not have enough staff to operate around the clock.
  - *Recruiting, hiring, and retaining security personnel.* One CISO stated that the agency could not offer salaries that are competitive with the private sector for candidates with high-demand technical skills. Another described a similar challenge, stating that the government's General Schedule system restricts agencies from offering bonuses commensurate with what private sector organizations can offer. Additionally, another respondent stated that, although hiring security personnel with less experience is cheaper than hiring at higher grades, the security organization has to devote significant time and effort to bringing new staff up to speed; additionally, once those staff obtain skills and experience, they often begin looking for new jobs where they can receive a higher salary.
  - *Expertise of security personnel.* CISOs described challenges with ensuring that personnel in highly technical roles have sufficient training opportunities and expertise in the skill sets needed. Others noted that a lack of expertise among staff limited their ability to evaluate risk, support internal testing, or oversee the security of IT acquisitions. Two noted that ISSOs at their agencies often are assigned these duties in addition to other responsibilities; others noted that ISSOs lack security skills or are not sufficiently trained. Another stated that the personnel supporting incident response at the agency had relatively little experience.
  - *Financial resources.* One CISO stated that the information security organization is funded through components' contributions to the department's working capital fund, which creates tension between the department-wide security needs and the operational priorities of the component agencies. Another stated that the CISO organization does not have a dedicated budget, but is funded out of the budget for the CIO organization. Another respondent stated that the CISO's ability to drive the agency to resolve POA&Ms in a timely manner is limited in part due to financial constraints. One respondent stated that his financial resources are insufficient for the human resources, training, and necessary tools and technologies needed to provide sufficient

---

oversight of security authorization decisions made by component agencies. Other CISOs stated that efforts to test security controls and remediate weaknesses are hampered due to budgetary constraints.

---

### Federal Efforts Are Under Way to Address Selected Challenges, but OMB Has Not Issued Guidance Addressing Challenges to CISOs' Authority

In accordance with their statutory responsibilities under FISMA, OMB and NIST have taken steps to assist federal agencies in implementing information security activities, and have instituted initiatives that can assist federal agencies in addressing challenges related to human and financial resources. For example:

- **The National Initiative for Cybersecurity Education:** This is an interagency effort coordinated by NIST to improve cybersecurity education, including efforts directed at training, public awareness, and the federal cybersecurity workforce. This initiative is intended to support the federal government's evolving strategy for education, awareness, and workforce planning and provide a comprehensive cybersecurity education program.
- **Cybersecurity National Action Plan:** Announced by the White House in February 2016, the Cybersecurity National Action Plan is intended to foster long-term improvements in the cybersecurity across the federal government, the private sector, and individuals. Among other things, the plan announces (1) the establishment of the Commission on Enhancing National Cybersecurity, which is to make recommendations on actions to enhance cybersecurity awareness and protections throughout the private sector and at all levels of government, to protect privacy, to maintain public safety and economic and national security, and to empower Americans to take better control of their digital security; (2) the creation of the Federal Chief Information Security Officer position to drive cybersecurity policy, planning, and implementation across the federal government; (3) efforts to enhance cybersecurity education and training nationwide and hire more cybersecurity experts to secure federal agencies; and (4) a proposal for \$19 billion of funding for cybersecurity in fiscal year 2017, a 35 percent increase over fiscal year 2016.
- **Cybersecurity Strategy and Implementation Plan:** Issued in October 2015, the Cybersecurity Strategy and Implementation Plan was created as a result of the 30-day Cybersecurity Sprint initiated in June 2015. The plan is intended to identify and address critical cybersecurity gaps and emerging priorities, and make specific recommendations to address those gaps and priorities. The plan is to strengthen federal civilian cybersecurity through five objectives: (1)

---

prioritized identification and protection of high-value information and assets, (2) timely detection of and rapid response to cyber incidents, (3) rapid recovery from incidents when they occur and accelerated adoption of lessons learned from the Cybersecurity Sprint assessment, (4) recruitment and retention of cybersecurity workforce talent, and (5) efficient and effective acquisition and deployment of existing and emerging technology.

If effectively implemented, these initiatives should help address several of the challenges identified by CISOs, particularly those related to insufficient numbers of staff; recruiting, hiring, and retaining qualified staff; personnel expertise; and funding. However, they do not address concerns raised by CISOs regarding their authority to carry out their responsibilities.

Existing OMB Implementation Guidance Does Not Address New FISMA Requirements for Ensuring Senior Agency Officials Are Held Accountable

Recognizing the importance of oversight of agency-wide information security activities, in enacting FISMA 2014 Congress added two new requirements that agency heads ensure that (1) senior agency officials carry out their information security responsibilities and (2) all agency personnel are held accountable for complying with the agency-wide information security program.<sup>36</sup> Given CISOs' statutory responsibilities for ensuring that their agencies comply with the requirements of the law, it is vitally important to address the challenges to their authority that the CISOs have identified, such as ensuring that the agency appropriately considers security in operational decisions; coordinating with and overseeing security activities of component organizations, other offices, and contractors; and elevating security concerns to upper management.

According to OMB, recent guidance addresses the implementation of these new requirements. Specifically, OMB officials stated that the office's June 2015 memorandum<sup>37</sup> that provides implementation guidance for the recently enacted IT reform legislation, commonly referred to as the

---

<sup>36</sup>44 U.S.C. § 3554(a)(6) & (7).

<sup>37</sup>OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (June 10, 2015).

---

Federal Information Technology Acquisition Reform Act (FITARA),<sup>38</sup> addresses the CISO's role in ensuring that senior officials are held accountable because it is intended to strengthen the agency CIO's accountability and oversight for information security across the agency. They added that under FISMA, this accountability and involvement would necessarily be delegated to the agency CISO.

Officials also stated that OMB's efforts to oversee agencies' implementation of the requirements in the memo, including PortfolioStat sessions,<sup>39</sup> included discussions with agency CIOs and CISOs regarding whether they have been given appropriate authority. They further stated that the annual FISMA reporting instructions issued by the office contain guidance on how agencies can ensure that CISOs are assigned appropriate responsibility and authority to ensure that information security activities are implemented. Officials also stated that the CyberStat meetings—in which OMB and DHS meet with agency CIOs, CISOs, and other agency officials to discuss and assist in developing focused strategies for improving their agency's cybersecurity posture—focus on FISMA-related security metrics and issues where the CISO should be involved.

In July 2016, OMB issued its update to Circular A-130, *Managing Information as a Strategic Resource*. Among other things, the circular requires agencies to ensure that the CIO designates a senior agency information security officer to develop and maintain an agency-wide information security program in accordance with FISMA 2014. The circular reiterates the new FISMA 2014 requirement for agencies to implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide information security and privacy requirements and policies and specifies that this requirement be part of the agency-wide information security program.

---

<sup>38</sup>FITARA was enacted as federal information technology acquisition reform provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014). The law includes several requirements for strengthening IT management at federal agencies.

<sup>39</sup>PortfolioStat is an OMB initiative which requires agencies to conduct annual reviews of their IT investments and make decisions on eliminating duplication, among other things. In a PortfolioStat session, key stakeholders from the agency meet face-to-face with the Federal CIO for an evidence-based review of the agency's IT portfolio.

---

However, neither the FITARA implementation guidance, FISMA reporting instructions, nor CyberStat meetings provide guidance for federal agencies on how to implement the new FISMA 2014 requirements or the CISO's role in carrying them out, nor do they indicate that OMB is evaluating CISOs' authority. Furthermore, while the updated Circular A-130 restates the new requirement to ensure that all personnel are held accountable, it does not provide guidance clarifying how this requirement should be implemented. The lack of clarity about how agencies are expected to implement these new requirements further hinders CISOs' ability to address the challenges to their authority that they reported facing. Additional guidance from OMB addressing how agencies should ensure that officials carry out their responsibilities and personnel are held accountable for complying with the agency-wide information security program could assist CISOs in more effectively carrying out their duties in the face of numerous challenges.

---

## Conclusions

Defining the role of a federal agency CISO is key to ensuring that this official is able to ensure that agency-wide information security programs are developed, documented, and implemented. Most agencies documented the role of the agency CISO in ensuring the implementation of security program activities in their information security policies; however, most agencies also had gaps in policies defining their CISO's responsibilities, leaving it unclear what role, if any, these officials play in some aspects of agencies' information security programs. By not fully defining this role, agencies may be unable to ensure that their CISOs are able to effectively oversee the implementation of their information security programs.

Although federal law and agency policies vest CISOs with responsibility for ensuring that agency-wide information security programs are developed, documented, and implemented, many CISOs reported challenges to their authority to effectively carry out these responsibilities, such as difficulties in coordinating with component organizations or other offices, obtaining reliable and timely information from other entities within the agency, and an inability to raise concerns to agency leadership. They also cited concerns in having adequate staff with relevant expertise and sufficient resources to implement security requirements. These can limit CISOs' ability to effectively ensure that the information security program is implemented and that agency-wide information security risk is managed appropriately. Several government-wide initiatives that are under way can address issues related to staffing and financial resources if fully implemented. However, OMB's current implementation guidance

---

does not address how to implement the new FISMA 2014 requirements or the CISO's role in carrying them out, nor does it identify how OMB will evaluate the role of the CISO. Further guidance from OMB could assist agencies in making sure that CISOs have adequate authority and could help ensure that agencies are fully defining the role of the CISO with respect to all elements of their information security programs.

---

## Recommendations for Executive Action

To assist CISOs in carrying out their responsibilities, we recommend that the Director of OMB issue guidance for agencies' implementation of the FISMA 2014 requirements to ensure that (1) senior agency officials carry out information security responsibilities and (2) agency personnel are held accountable for complying with the agency-wide information security program. This guidance should clarify the role of the agency CISO with respect to these requirements, as well as implementing the other elements of an agency-wide information security program, taking into account the challenges identified in this report.

We are also making 33 recommendations to 13 of the 24 departments and agencies in our review to ensure that the role of the CISO is defined in agency policy in accordance with FISMA. Appendix II contains these recommendations.

---

## Agency Comments and Our Evaluation

We provided a copy of a draft of this report to OMB and all 24 departments and agencies for review and comment. We received written comments from 12 agencies which are reprinted in appendices III through XIV. We received comments by email from 5 agencies and no comments from the remaining agencies. We also received technical comments from three agencies that we incorporated into the report as appropriate.

Of the 13 agencies to which we made specific recommendations, 12 concurred with our recommendations and 9 identified steps that they are taking or plan to take to address them. One agency, DOD, did not concur or partially concurred with the three recommendations we made to it. For a summary of each of the 13 agencies' comments and our response, please see appendix II.

In comments provided via e-mail on July 29, 2016, by OMB's audit liaison in the Office of General Counsel, OMB stated that it partially concurred with our recommendation. OMB also stated that it believes that its annual FISMA 2014 guidance provides sufficient and clear details on the expectations for agencies, to include procedures for overseeing and

---

managing their information security programs, and that the guidance incorporates agency feedback and information security best practices to better reflect challenges and solutions within the current government operating environment. OMB noted that developing prescriptive guidance to address or streamline variances in information security management practices may unintentionally hamper agencies' ability to conduct their missions. It added that, in place of issuing such guidance, OMB plans to continue utilizing several oversight mechanisms to drive performance and address challenges, including quarterly FISMA performance reviews and face-to-face CyberStat Reviews.

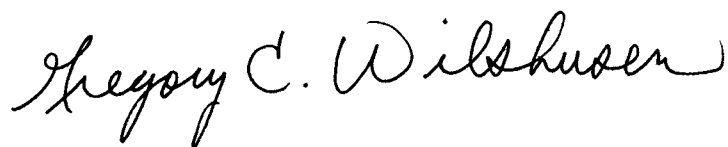
We disagree that existing guidance and oversight mechanisms provide sufficient clarity for agencies on how to implement the new FISMA 2014 provisions. As stated in this report, neither the annual FISMA guidance nor CyberStat meetings provide guidance for federal agencies on how to implement the new FISMA 2014 requirements or the CISO's role in carrying them out. In addition, OMB's recently revised Circular A-130 is clear that the CISO is to have a role in ensuring that all personnel are held accountable for complying with information security requirements, but it does not provide guidance on how agencies are to implement this requirement. As we note in our report, CISOs are not always able to effectively hold personnel accountable for complying with information security requirements. Accordingly, additional guidance from OMB addressing how agencies should ensure that officials carry out their responsibilities and personnel are held accountable for complying with the agency-wide information security program could help address many of the challenges to authority identified by federal CISOs. We therefore believe our recommendation is warranted.

---

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees, the Director of the Office of Management and Budget, the secretaries and agency heads of the departments and agencies addressed in this report, and other interested parties. In addition, this report will be available at no charge on the GAO website at <http://www.gao.gov>.

---

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

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent "G" and "W".

Gregory C. Wilshusen  
Director, Information Security Issues



---

# Appendix I: Objectives, Scope, and Methodology

---

Our objectives were to (1) identify the key responsibilities of federal chief information security officers (CISO) established by federal law and guidance and determine the extent to which federal agencies have defined the role of the CISO in accordance with this law and guidance and (2) describe key challenges of federal agency CISOs in fulfilling their responsibilities to ensure that agency-wide information security programs are developed, documented, and implemented. The scope of our review included the 24 major departments and agencies covered by the Chief Financial Officers Act of 1990.<sup>1</sup>

To identify the key responsibilities of federal CISOs established by federal law and guidance, we reviewed relevant laws including relevant provisions of the Federal Information Security Management Act of 2002 (FISMA 2002), the Federal Information Security Modernization Act of 2014 (FISMA 2014) and the Federal Information Technology Acquisition Reform Act (FITARA). In addition, we reviewed relevant special publications from the National Institute of Standards and Technology (NIST) addressing information security management topics and Office of Management and Budget (OMB) memoranda and circulars addressing federal information security.

To determine the extent to which federal agencies have defined the role of the CISO in accordance with law and guidance, we collected information security policies and procedures from the 24 major departments and agencies. We then evaluated each agency's policies to determine responsibility for ensuring that information security activities are implemented had been assigned to the CISO in accordance with FISMA 2014. In addition, we collected and reviewed each agency's current organization chart(s) depicting the CISO's position relative to the head of the agency, other senior officials, and component CISOs, if applicable. We also asked each agency to supply the name of each of the individuals who had served as CISO at the agency since 2010.

---

<sup>1</sup>The 24 major federal agencies covered by the Chief Financial Officers Act of 1990 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; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

To describe key challenges of federal agency CISOs in exercising their authority to ensure that agency-wide information security programs are developed, documented, and implemented, we developed and administered a web-based survey instrument to the CISO at each of the 24 major departments and agencies in coordination with our survey methodology expert. In the survey, we asked CISOs to identify whether they felt that they had sufficient levels of responsibility and authority. In addition, we asked CISOs to identify factors that challenged them in exercising their authority, and to identify specific challenges related to these factors. We then reviewed the responses provided by the CISOs and interviewed each of them in order to validate responses from the survey and to obtain additional insight into the challenges they identified. From the survey and interview responses, we analyzed CISOs' comments to identify challenges common across multiple agencies.

To minimize errors that might occur from respondents interpreting our questions differently from our intended purpose, we pretested the questionnaire in person and by phone with the CISOs at three agencies. The selection of agencies for pretesting was based on agency availability to assist us with pretesting, variation in size of agency, and variation in agency security governance models (i.e., centralized or decentralized). During these pretests, we asked each CISO to complete the survey as we listened to the process. We then interviewed the respondents to check whether the questions were applicable, clear, unambiguous, and easy to understand. We then revised the survey based on the feedback provided during the pretests prior to sending the final survey to the agency CISOs. All 24 Chief Financial Officers Act agency CISOs completed the final survey, although not all survey respondents answered every question.

The practical difficulties of conducting any survey may introduce non-sampling errors. For example, differences in how a particular question is interpreted, the sources of information available to respondents, or the types of respondents who do not respond to a question can introduce errors into the survey results. We included steps in both the data collection and data analysis stages to minimize such non-sampling errors. We examined the survey results and performed computer analyses to identify inconsistencies and other indications of error, and addressed such issues as necessary. We analyzed responses to closed-ended questions by counting the responses for all agencies. For questions that asked respondents to provide a narrative answer, we compiled the answers in one spreadsheet that was analyzed and used as examples in the report.

To assess any OMB efforts to provide guidance on the implementation of new FISMA 2014 requirements for agencies to ensure that senior officials carry out their responsibilities and to hold personnel accountable, we analyzed OMB memoranda establishing requirements for federal information security to determine whether they addressed matters of information security governance and the role of the CISO. We also met with representatives from OMB to obtain their views on the new FISMA requirements, the role of CISOs in carrying them out, and the role of OMB in providing guidance for agencies in implementing the new requirements.

We conducted this performance audit from June 2015 to August 2016 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: Recommendations to Departments and Agencies

---

## Department of Commerce

To ensure that the role of the chief information security officer (CISO) is defined in department policy in accordance with the Federal Information Security Modernization Act of 2014 (FISMA 2014), we recommend that the Secretary of Commerce take the following action:

- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.

In its comments on a draft of this report, the Department of Commerce concurred with our recommendation and stated that it planned to update the department's IT policy and program documents that define the roles and responsibilities of the CISO by September 30, 2017, with progress to be tracked quarterly. The department's comments are reprinted in appendix III. The department also provided technical comments which we have incorporated into the final report as appropriate.

---

## Department of Defense

To ensure that the role of the senior information security officer (SISO) is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of Defense take the following three actions:

- Define the SISO's role in department policy for ensuring that information security policies and procedures are developed and maintained.
- Define the SISO's role in department policy for ensuring that the department has procedures for incident detection, response, and reporting.
- Define the SISO's role in department policy for oversight of security for information systems that are operated by contractors on the department's behalf.

In its comments on a draft of this report, DOD stated that it did not concur with the first recommendation and partially concurred with the other two.

Our draft report included five additional recommendations to DOD: that the department define the SISO's role in department policy (1) for ensuring that subordinate security plans are documented for the department's information systems; (2) for ensuring that security controls are tested periodically; (3) for ensuring that the department has a process for planning implementing, evaluating, and documenting remedial actions; (4) for ensuring that plans and procedures are in place to ensure recovery

and continued operations of the department's information systems in the event of a disruption, and (5) in the periodic authorization of the department's information systems. DOD did not concur with four of these draft recommendations and partially concurred with one of them. DOD stated that the SISO organization maintains a knowledge service that provides component organizations with DOD-specific assignment values for contingency planning security controls, implementation guidance, and assessment procedures, and that the department's risk management framework policy defines the SISO's role in security planning, security control testing, remedial actions, and system authorization activities. We reviewed DOD's cybersecurity instruction and risk management framework policy and confirmed that the department's statements are accurate. Therefore, we have made appropriate changes in the report to reflect this information, including withdrawing these five recommendations from the final report.

DOD did not concur with our recommendation that the department define the SISO's role in department policy for ensuring that information security policies and procedures are developed and maintained. The department's response stated that according to the DOD cybersecurity instruction, the SISO is responsible for directing and coordinating the DOD cybersecurity program and carrying out the CIO's responsibilities in accordance with FISMA 2014; accordingly, the SISO is responsible for developing and maintaining information security policies as stated in FISMA 2014. The department also noted that it had provided us with an organization chart showing that the DOD SISO organization included a cybersecurity policy division. However, we still believe that the SISO's role with respect to information security policies and procedures is not sufficiently defined. This is because neither the cybersecurity instruction nor any other policy document provided to us described any specific responsibilities of the SISO in ensuring that information security policies and procedures are developed and maintained, nor did they describe the responsibilities of the cybersecurity policy division. The SISO is the official with responsibility for directing and coordinating the department's cybersecurity program. Therefore, it is important that the SISO's role in ensuring that information security policies and procedures are developed and maintained be clearly defined in DOD policy. We therefore believe that our recommendation is warranted.

DOD partially concurred with our recommendation that it define the SISO's role in department policy for ensuring that the department has procedures for incident detection, response, and reporting. The department stated that responsibility for managing the incident handling

program has been assigned to Cyber Command within U.S. Strategic Command by the Secretary of Defense, and that the department's incident handling program is documented in Chairman of the Joint Chiefs of Staff Manual 6510.01 B, "Cyber Incident Handling Program." The department also noted that the SISO organization plans to publish a new cyber incident handling manual to replace the existing Chairman of the Joint Chiefs of Staff Manual. It will be important for the new manual to clearly define the role of the SISO in the incident handling process. We therefore continue to believe that our recommendation is warranted.

DOD partially concurred with our recommendation that it define the SISO's role in department policy for oversight of contractor system security, and stated that the SISO organization has developed and maintains policies providing direction to DOD components on oversight of contractor system security, including policies on defense industrial base cyber security/information assurance activities and on the security of unclassified DOD information on non-DOD information systems. DOD also stated that the SISO will review the CIO and component SISO responsibilities in the regularly scheduled updates to these policies. The department further stated that its national industrial security program operating manual describes that the Director of the Defense Security Service monitors and oversees information security practices of contractors and vendors processing classified DOD information, and that the Defense Federal Acquisition Regulation Supplement Subpart 204.73 requires contractors to implement security requirements.

However, neither the policies on defense industrial base cyber security/information assurance activities or the security of unclassified DOD information on non-DOD information systems, the national industrial security program operating manual, nor the Defense Federal Acquisition Regulation Supplement specify any roles or responsibilities for the DOD SISO in the area of contractor system security. While it may be appropriate to review the responsibilities of the DOD CIO and component SISOs, because the SISO is the official with responsibility for directing and coordinating the department's cybersecurity program, it is important that the responsibilities of the SISO in overseeing the security of contractor systems be clearly defined in DOD policy. We therefore believe that our recommendation is warranted.

DOD's comments are reprinted in appendix IV.

---

## Department of Energy

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of Energy take the following six actions:

- Define the CISO's role in department policy for ensuring that subordinate security plans are documented for the department's information systems.
- Define the CISO's role in department policy for ensuring that all users receive information security awareness training.
- Define the CISO's role in department policy for ensuring that the department has a process for planning implementing, evaluating, and documenting remedial actions.
- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.
- Define the CISO's role in department policy for oversight of security for information systems that are operated by contractors on the department's behalf.
- Define the CISO's role in department policy in the periodic authorization of the department's information systems.

In its comments on a draft of this report, DOE concurred in principle with our recommendations, and stated that it is meeting implementation requirements as stated in FISMA 2014 through delegation memoranda and other supporting directives in a manner that supports the department's diverse missions while focusing on ensuring an enterprise-wide approach to cyber security. The department also agreed that further codification of the role of the CISO is appropriate within department policies. DOE stated that it is undertaking a review of its cybersecurity program order and will consider GAO's recommendations during that process.

Our draft report also included three additional recommendations that the agency define the CISO's role in department policy for ensuring that (1) information security policies and procedures are developed and maintained, (2) security controls are tested periodically, and (3) personnel with significant security responsibilities receive appropriate training. Subsequently, DOE provided additional documentation demonstrating that the CISO's role for these activities has been defined. As a result, we have withdrawn these three recommendations associated with these activities and made appropriate changes in the report to reflect the updated information. The department's comments are reprinted in

appendix V. The department also provided technical comments which we have incorporated into the final report as appropriate

---

## Department of Health and Human Services

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of Health and Human Services take the following action:

- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.

In its comments on a draft of this report, HHS concurred with our recommendation and stated that the updates to policy are to be made in conjunction with anticipated revisions of NIST SP 800-53, revision 5. The department's comments are reprinted in appendix VI.

---

## Department of the Interior

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of the Interior take the following four actions:

- Define the CISO's role in department policy for ensuring that subordinate security plans are documented for the department's information systems.
- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.
- Define the CISO's role in department policy for oversight of security for information systems that are operated by contractors on the department's behalf.
- Define the CISO's role in department policy in the periodic authorization of the department's information systems.

In its comments on a draft of this report, the Department of the Interior concurred with our four recommendations and stated that it is currently updating policy to ensure that they are implemented. The department's comments are reprinted in appendix VIII.

---

## Department of Justice

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Attorney General take the following two actions:



- Define the CISO's role in department policy for ensuring that information security policies and procedures are developed and maintained.
- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.

In its comments on a draft of this report, DOJ concurred with our recommendations and stated that the department has clarified the CISO responsibilities in a revised policy which is expected to be released in August 2016. The department's comments are reprinted in appendix IX.

---

## Department of State

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of State take the following action:

- Define the CISO's role in department policy for ensuring that the department has procedures for incident detection, response, and reporting.

In its comments on a draft of this report, the Department of State stated that it concurred with our finding and plans to correct policy guidance to reflect that the Security Infrastructure/Cybersecurity/ Monitoring and Incident Response Division within the Bureau of Diplomatic Security is the entity responsible for incident response. Further, it stated that the bureaus of Information Resource Management and Diplomatic Security are continuing to work to further coordinate communications for incident response. The department's comments are reprinted in appendix X.

---

## Department of Transportation

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of Transportation take the following two actions:

- Define the CISO's role in department policy for ensuring that subordinate security plans are documented for the department's information systems.
- Define the CISO's role in department policy for ensuring that security controls are tested periodically.

In comments on a draft of this report provided via e-mail on July 22, 2016, by an Audit Relations Analyst in DOT's Audit Relations and Program Improvement office, the department stated that it concurred with the findings and recommendations in our report.

---

Department of the  
Treasury

To ensure that the role of the CISO is defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of the Treasury take the following seven actions:

- Define the CISO's role in department policy for ensuring that subordinate security plans are documented for the department's information systems.
- Define the CISO's role in department policy for ensuring that all users receive information security awareness training.
- Define the CISO's role in department policy for ensuring that security controls are tested periodically.
- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.
- Define the CISO's role in department policy for ensuring that personnel with significant security responsibilities receive appropriate training.
- Define the CISO's role in department policy for oversight of security for information systems that are operated by contractors on the department's behalf.
- Define the CISO's role in department policy in the periodic authorization of the department's information systems.

In comments on a draft of this report provided via e-mail on August 3, 2016, a representative from Treasury's Office of the Associate CIO stated that Treasury concurred with our recommendations. The department also provided technical comments which we have incorporated into the final report as appropriate.

---

Environmental Protection  
Agency

To ensure that the role of the senior agency information security officer (SAISO) is defined in agency policy in accordance with FISMA 2014, we recommend that the Administrator of the Environmental Protection Agency take the following three actions:

- Define the SAISO's role in agency policy for ensuring that subordinate security plans are documented for the department's information systems.
- Define the SAISO's role in agency policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.
- Define the SAISO's role in agency policy in the periodic authorization of the department's information systems.

In its comments on a draft of this report, the Environmental Protection Agency agreed with our report's recommendations and stated that the agency expected to implement them by July 29, 2016. The agency's comments are reprinted in appendix XI.

---

### National Aeronautics and Space Administration

To ensure that the role of the SAISO is defined in agency policy in accordance with FISMA 2014, we recommend that the Administrator of the National Aeronautics and Space Administration take the following action:

- Define the SAISO's role in agency policy for oversight of security for information systems that are operated by contractors on the agency's behalf.

In its comments on a draft of this report, NASA concurred with our recommendation and stated that the agency expects to implement it by December 9, 2016. NASA's comments are reprinted in appendix XII.

---

### Small Business Administration

To ensure that the role of the CISO is defined in agency policy in accordance with FISMA 2014, we recommend that the Administrator of the Small Business Administration take the following action:

- Define the CISO's role in agency policy for ensuring that personnel with significant security responsibilities receive appropriate training.

In comments on a draft of this report provided via e-mail on July 22, 2016, a program manager in SBA's Office of Congressional and Legislative Affairs stated that the agency agreed with our recommendation and had no comments on the report.

---

### U.S. Agency for International Development

To ensure that the role of the CISO is defined in agency policy in accordance with FISMA 2014, we recommend that the Administrator of the U.S. Agency for International Development take the following action:

- Define the CISO's role in agency policy for oversight of security for information systems that are operated by contractors on the agency's behalf.

In its comments on a draft of this report, USAID agreed with our recommendation and stated that the Office of the Administrator, in coordination with the Office of the Chief Information Officer, will update operational policy to define the CISO's role for oversight of contractor system security. The agency's comments are reprinted in appendix XIII.

# Appendix III: Comments from the Department of Commerce



THE DEPUTY SECRETARY OF COMMERCE  
Washington, D.C. 20230

July 26, 2016

Mr. Gregory Wilshusen  
Director, Information Technology Security Issues  
Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority* (GAO-16-686).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. We have concurred with the recommendation, and we will ensure that the Department defines the Chief Information Security Officer's (CISO) role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption. We will do this by updating Commerce IT policy and program documents that define the roles and responsibilities of the CISO. We will ensure that these documents are updated by the end of the 4th Quarter, FY 2017, and the progress of this effort will be tracked quarterly.

We will also proceed to update our internal policies, should guidance be released by the Office of Management and Budget, per recommendations made by GAO to clarify CISO's roles in light of identified challenges. If you have any questions, please contact Steve Cooper, Chief Information Officer at the Department of Commerce, at (202) 482-4797.

Sincerely,

A handwritten signature in black ink, appearing to read "B. H. Andrews", is written over a horizontal line.

Bruce H. Andrews

Enclosure

Department of Commerce  
Office of the Chief Information Officer  
Office of the Secretary

Technical and Editorial Comments on the  
Government Accountability Office Draft Report Titled  
*Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and  
Address Challenges to Authority (GAO-16-686)*

The Office of the Chief Information Officer has reviewed the draft report, and our technical and editorial comments are below. Page numbers refer to page numbers in the report unless otherwise stated.

**General Comments**

The report is reasonable, and we concur with its findings and recommendations.

**Recommended Changes for Factual/Technical Information.**

None.

**Editorial Comments**

None.

# Appendix IV: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

**DEPARTMENT OF DEFENSE**  
8000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-6000

Mr. Gregory Wilshusen  
Director, Information Technology  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Wilshusen:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-16-686, "FEDERAL CHIEF INFORMATION SECURITY OFFICERS: Opportunities Exist to Improve Roles and Address Challenges to Authority," dated June 30, 2016 (GAO Code 100105).

We acknowledge receipt of the draft report and note that the GAO makes eight recommendations to the Department on page 40 of the report. In response to your request we provide the attached document. The DoD CIO nonconcur with five recommendations and partially concurs with three recommendations.

Should you have any questions, please contact Mr. David C. Myers, 703-571-5811, david.c.myers.civ@mail.mil.

Sincerely,

A handwritten signature in cursive script that reads "David L. De Vries". To the right of the signature, the date "5 Aug 2016" is written in a smaller, less legible script.

David L. De Vries  
Principal Deputy

Attachment:  
As stated

GAO DRAFT REPORT DATED JUNE 30, 2016  
GAO-16-686 (GAO CODE 100105)

**"FEDERAL CHIEF INFORMATION SECURITY OFFICERS: OPPORTUNITIES  
EXIST TO IMPROVE ROLES AND ADDRESS CHALLENGES TO AUTHORITY"**

**DEPARTMENT OF DEFENSE COMMENTS  
TO THE GAO RECOMMENDATION**

**BACKGROUND:**

1. The functions of the Department of Defense (DoD) and its major Components are established in DoD Directive (DoDD) 5100.01, "Functions of the Department of Defense and Its Major Components." All functions in the Department of Defense are performed under the authority, direction, and control of the Secretary of Defense.
2. DoDD 5144.02, "DoD Chief Information Officer (DoD CIO)" signed by the Deputy Secretary of Defense under the authority vested in the Secretary of Defense by section 113 of Title 10, United States Code (U.S.C.) assigns the responsibilities functions, relationships, and authorities of the DoD CIO.
  - a. This directive assigns the DoD CIO the responsibility for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems; cybersecurity; positioning, navigation, and timing (PNT) policy, and the DoD information enterprise that supports DoD command and control (C2).
  - b. This directive authorizes the DoD CIO, as the Principal Staff Assistant (PSA) reporting directly to the Secretary of Defense, to establish DoD policy in DoD issuances within the responsibilities, functions, and authorities assigned in this directive.
3. DoDD 8000.01, "Management of Department of Defense Information Enterprise" signed by the Deputy Secretary of Defense establishes and defines roles for DoD Component CIOs for ensuring that Components comply with, and promptly, and effectively implement the policies and responsibilities in the directive and Federal Information Security Modernization Act of 2014 (FISMA 2014) requirements.
4. The DoD CIO as the PSA for cybersecurity, through the Deputy CIO for Cybersecurity/ Senior Information Security Officer (DCIO(CS)/SISO), and the subordinate DoD CIO Office of the Director for Cybersecurity Policy, Strategy, and Workforce develops and maintains policy and standards for the Defense cybersecurity program through DoD issuances.
5. These issuances establish the responsibilities, functions, and authorities of DoD Component Heads, DoD Component appointed CIOs, and appointed SISOs to implement the DoD Components' cybersecurity program; and protect the DoD Components' systems under their authority or operating on their behalf in accordance with FISMA 2014 requirements.

6. The responsibility for DoD-level policy and oversight of the overall Defense cybersecurity (information security) program is assigned to the DoD CIO as a PSA and to the DoD SISO. However, DoD Components (e.g., 3 Military Departments, Joint Chiefs of Staff, 9 combatant commands, 18 Defense Agencies, 10 DoD Field Activities) are assigned the responsibility to implement the Defense cybersecurity program and the systems within their Component under the oversight of their CIO and SISO. DoD also assigns responsibilities, functions, relationships, and authorities to USSTRATCOM and USCYBERCOM and Military Service forces to protect DoD information networks through the cyberspace operations command and control framework.

**RECOMMENDATION 1:** The GAO recommends that the Secretary of Defense define the senior information security officer's (SISO) role in department policy for ensuring that information security policies and procedures are developed and maintained.

**DoD RESPONSE:** DoD nonconcur with recommendation 1. The role and responsibilities of the DoD SISO are clearly identified in DoD Instruction (DoDI) 8500.01, "Cybersecurity." The DoDI 8500.01 states, "Directs and coordinates the Defense cybersecurity program and , as delegated, carries out the DoD CIO's responsibilities pursuant to 44 USC 3554. As such, the DCIO(CS)/DoD SISO develops and maintains information security policies as stated in section 3554 of Title 44 and in accordance with DoDD 5144.02, "DoD Chief Information Officer (DoD CIO)." Additionally, GAO received a DCIO Cybersecurity/DoD SISO organization chart identifying Cybersecurity Policy division under the DoD SISO.

**RECOMMENDATION 2:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy for ensuring that subordinate security plans are documented for the department's information systems.

**DoD RESPONSE:** DoD nonconcur with recommendation 2. The DoD SISO is assigned the role to establish and maintain the risk management framework (RMF) in DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" which states: "DoD SISO, in accordance with DoDI 8500.01, "Cybersecurity", represents the DoD CIO and directs and coordinates the DoD Cybersecurity Program, which includes the establishment and maintenance of the RMF." The RMF security plan requirements are outlined in DoDI 8510.01, including the requirement for system security plans and their documentation as part of an authorization package: The instruction also assigns the DoD Components responsibility to: "The DoD Components will develop and implement processes whereby the AO [*authorizing official*] (or designee) reviews and approves the security plan and system-level continuous monitoring strategy submitted by the ISO [*information security officer*] or PM/SM [*program manager/system manager*]...The AO approval of the security plan must be documented in the security plan." The DCIO(CS)/DoD SISO also maintains the RMF Knowledge Service to provide DoD-specific assignment values for security controls, implementation guidance, and assessment procedures for use by DoD Component organizations. As such, the DCIO(CS)/DoD SISO develops and maintains information security policies as stated in section 3554 of Title 44 for the Agency information systems to document of security plans.

**RECOMMENDATION 3:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy for ensuring that security controls are tested periodically.



**DoD RESPONSE:** DoD nonconcur with recommendation 3. The DoD SISO is assigned the role to establish and maintain the RMF in DoDI 8510.01 which states: "DoD SISO, in accordance with DoDI 8500.01, "Cybersecurity", represents the DoD CIO and directs and coordinates the DoD Cybersecurity Program, which includes the establishment and maintenance of the RMF." DoDI 8510.01 assigns DoD Components Heads the responsibility to ensure DoD information technologies under their authority comply with the RMF. DoDI 8510.01 requires, program managers or system managers to: "Ensure periodic reviews, testing and assessment of assigned IS and PIT systems are conducted at least annually." The DCIO(CS)/DoD SISO also maintains the RMF Knowledge Service to provide DoD-specific assignment values for continuous monitoring and testing related security controls, implementation guidance, and assessment procedures for use by DoD Component organizations. As such, the DCIO(CS)/DoD SISO develops and maintains information security policies as stated in section 3554 of Title 44 for Agency periodic testing of security controls.

**RECOMMENDATION 4:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy for ensuring that the department has a process for planning implementing, evaluating, and documenting remedial actions.

**DoD RESPONSE:** DoD nonconcur with recommendation 4. The DoD SISO is assigned role to establish and maintain the RMF in DoDI 8510.01 which states: "DoD SISO, in accordance with DoDI 8500.01, "Cybersecurity", represents the DoD CIO and directs and coordinates the DoD Cybersecurity Program, which includes the establishment and maintenance of the RMF. DoDI 8510.01 assigns DoD Component Heads are responsible to ensure DoD information technologies under their authority comply with the RMF. Enclosure 6, "Risk Management of IS and PIT Systems," provides the RMF process and DoD Component responsibilities to implement security controls, assess security controls, document the assessment in the security assessment report (SAR) of the plan of action and milestones (POA&M). The policy also requires that the SAR documents address security controls in a non-compliance status, including existing and planned mitigations. The guidance also requires that the DoD Component CIO forward authorization decisions and supporting rationale for those systems with non-compliant security controls with a level of "Very High" or "High" to the DoD Information Security Risk Management Committee and DoD SISO. As such, the DCIO(CS)/DoD SISO develops and maintains information security policies as stated in section 3554 of Title 44 for Agency periodic testing of security controls.

**RECOMMENDATION 5:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy for ensuring that the department has procedures for incident detection, response, and reporting.

**DoD RESPONSE:** DoD partially concurs with recommendation 5. The DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations" requires DoD Components to establish a cyber incident handling program with capability to analyze and respond to events or cyber incidents to mitigate any adverse operational or technical impact on the DoD Component-owned or -operated portion of the DoD information network (DoDIN) in accordance with Chairman Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program." This manual describes the DoD Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related U.S. government interactions. United States Cyber Command (USCYBERCOM) as a sub-unified command of United States Strategic Command

(USSTRATCOM) is responsible for managing the incident handling program and has been assigned directive authority for cyberspace operations to issue orders to DoD Components to assure the effective functioning and defense of the entire DoDIN by the Secretary of Defense. The DCIO(CS)/DoD SISO will be updating and publishing a new DoD manual on cyber incident handling to replace the CJCS manual with the DCIO(CS)/DoD SISO maintaining information security policies as stated in section 3554 of Title 44 for Agency cyber incident handling procedures for incident detection, response, and reporting.

**RECOMMENDATION 6:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information system in the event of a disruption.

**DoD RESPONSE:** DoD partially concurs with recommendation 6. DoDI 8500.01 assigns the responsibility to the DoD Component Heads to develop DoD IS contingency plans and conduct exercises to recover information systems following an emergency or information system disruption using guidance found in NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems." The DCIO(CS)/DoD SISO also maintains the RMF Knowledge Service to provide DoD-specific assignment values for contingency planning security controls, implementation guidance, and assessment procedures for use by DoD Component organizations. In future reviews, DoDI 8500.01 and DoDI 8510.01 will be examined to determine if changes are required to the SISO role in maintaining information security policies as stated in section 3554 of Title 44 to ensure DoD Component plans and procedures are in place for recovery and continued operations of the DoD Component information systems in the event of a disruption.

**RECOMMENDATION 7:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy for oversight of contractor system security.

**DoD RESPONSE:** DoD partially concurs with recommendation 7. DCIO (CS)/SISO has developed and maintains issuances providing direction to DoD Components on oversight of contractor system security. These include the following, DoDI 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities" establishes policy, assigns responsibilities, and delegates authority for directing the conduct of DIB CS/IA activities to protect unclassified DoD information that transits or resides on unclassified DIB information systems and networks. DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems" establishes policy for managing the security of unclassified DoD information on non-DoD information systems. The Director Defense Security Service (DSS) monitors and oversees information security practices of DoD cleared defense contractors and vendors processing classified DoD information in accordance with DoD 5220.22-M, "National Industrial Security Program Operating Manual." In the regularly schedule updates to these issuances, the DCIO(CS)/DoD SISO will include review of DoD CIO and DoD Component SISO responsibilities to support the department's policy for oversight of contractor system security. DoD has also published revised Defense Federal Acquisition Regulation Supplement Part 204, Subpart 204-73, "Safeguarding Covered Defense Information and Cyber Incident Reporting," which applies to contracts and subcontracts and implementation of the security requirements specified by National Institute of Standards and Technology (NIST) Special

Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

**RECOMMENDATION 8:** The GAO recommends that the Secretary of Defense define the SISO's role in department policy in the periodic authorization of the department's information systems.

**DoD RESPONSE:** DoD nonconcur with recommendation 8. The DoD SISO is assigned the role to establish and maintain the RMF in DoDI 8510.01 which states: "DoD SISO, in accordance with DoDI 8500.01, "Cybersecurity", represents the DoD CIO and directs and coordinates the DoD Cybersecurity Program, which includes the establishment and maintenance of the RMF. DoDI 8510.01 states the DoD Component Heads are responsible to: "Ensure DoD information technologies under their authority comply with the RMF." Enclosure 6, "Risk Management of IS and PIT Systems," requires the AO to reviews the reported security status of the system on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the nation remains acceptable. In accordance with Appendix III to OMB Circular A-130, DoDI 8510.01 requires systems to be reassessed and reauthorized once every 3 years. The results of an annual review or a major change in the cybersecurity posture at any time may also indicate the need for reassessment and reauthorization of the system. The guidance also requires that the DoD Component CIO forward authorization decisions and supporting rationale for those systems with non-compliant security controls with a level of "Very High" or "High" to the DoD Information Security Risk Management Committee and DoD SISO. As such, the DCIO(CS)/DoD SISO develops and maintains information security policies as stated in section 3554 of Title 44 for Agency periodic authorization of the DoD Component's information systems.

# Appendix V: Comments from the Department of Energy



## Department of Energy

Washington, DC 20585

July 29, 2016

Mr. David A. Powner  
Director, Information Technology and Management Issues  
U.S. Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20548

Dear Mr. Powner:

I am pleased to provide the Department of Energy's (DOE) response to the Government Accountability Office's (GAO) Draft Report GAO-16-686 (job code 100105) titled *Federal Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*. The Department appreciates the opportunity to review the report prior to publication.

The Department concurs in principle with the GAO recommendations. While DOE agrees with the Draft Report GAO-16-686 regarding the need for clarification of the responsibilities and authorities assigned to the Chief Information Security Officer (CISO) in Department policy, the Department is meeting implementation requirements as stated in the Federal Information Security Modernization Act of 2014 (FISMA) through delegation memoranda, and other supporting directives. DOE implements FISMA in a manner that supports the diverse DOE missions while focusing on ensuring an enterprise-wide approach to cyber security. The Department agrees that further codification of the role of the CISO is appropriate within Department policies.

DOE is undertaking a review of DOE Order 205.1B, Department of Energy Cyber Security Program. During this review, the Department will consider the GAO recommendations. Further, DOE will consider future guidance from the Office of Management and Budget (OMB) guidance regarding CISO responsibilities.

Enclosure 1 includes additional details regarding DOE's response. Enclosure 2 contains technical comments that recommend changes to the Draft Report GAO-16-686.

Kindly direct your questions to Mr. Paul Cunningham, CISO, Office of the Chief Information Officer, Department of Energy at (202) 286-0166 or via e-mail to [Paul.Cunningham@hq.doe.gov](mailto:Paul.Cunningham@hq.doe.gov).

Sincerely,

A handwritten signature in black ink, appearing to read "Michael Johnson", is written over a horizontal line.

Michael Johnson  
Chief Information Officer

Enclosures



Enclosure 1

MANAGEMENT RESPONSE  
GAO Draft Report, GAO-16-686  
FEDERAL INFORMATION SECURITY OFFICERS: OPPORTUNITIES EXIST TO  
IMPROVE ROLES AND ADDRESS CHALLENGES TO AUTHORITY

Each recommendation in this report calls on the Chief Information Officer (CIO) to define the Chief Information Security Officer's (CISO's) role in Department policy in various ways. Currently, the Secretary of Energy delegates FISMA 2014 responsibilities to the CIO pursuant to DOE Redesignation Order No. 00-002.14. The CIO further designates these FISMA 2014 responsibilities and authority to the CISO through DOE Designation Order No. 00-28.00. Additionally, DOE O 205.1B, Department of Energy Cyber Security Program reinforces CISO responsibilities, including those defined by FISMA.

The Department concurs in principle with the GAO Draft Report, GAO-16-686 and agrees that clarification of the responsibilities and authorities assigned to the CISO is needed in Department policy. Each of the following management decisions describes how the Department is currently defining the CISO's FISMA role and how the Department plans to further codify the authority of the CISO's role in Department policies.

**Recommendation 1:**

*Define the CISO's role in department policy for ensuring that information security policies and procedures are developed and maintained.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 currently defines the CISO's role in Department policy for ensuring that information security policies and procedures are developed and maintained.

DOE Designation Order No. 00-28.00, section 1.A.2 states that "The CISO is responsible for developing and maintaining information security policies, procedures, and control techniques." Also, section 1.A.4.(c) states that "the CISO will assist other senior DOE officials concerning their responsibilities to provide information security, including implementation of policies and procedures."

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 2:**

*Define the CISO's role in Department policy for ensuring that subordinate security plans are documented for the Department's information systems.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 currently defines the CISO's role in Department policy for ensuring Departmental Elements document subordinate security plans for the Department's information systems.

DOE Designation Order No. 00-28.00, section 1.A.4.(d), states that "The CISO is responsible for assisting senior DOE officials concerning their responsibilities to provide information security for the information and information systems that support the operations and assets under their control including through periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented." Although not explicitly stated, this responsibility includes the CISO ensuring that Departmental Elements document subordinate security plans for the Department's information systems.

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 3:**

*Define the CISO's role in Department policy for ensuring that all users receive information security awareness training.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 and DOE O 205.1B currently define the CISO's role in Department policy for ensuring that all users receive information security awareness training.

DOE Designation Order No. 00-28.00, paragraph 1.A.3 directs that "The CIO and his designee (CISO) have responsibilities for training and overseeing personnel with significant information security responsibilities."

In the DOE O 205.1B, Section 1.d. states that, "A core requirement of the DOE's Risk Management Approach (RMA) is requiring a training, education, and awareness program." In addition, DOE O 205.1B, Sections 5.d and 5.e, states that "The CIO and CISO have responsibility for maintaining the Department's RMA." DOE requires annual information security awareness training.

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 4:**

*Define the CISO's role in Department policy for ensuring that security controls are tested periodically.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 currently defines the CISO's role in Department policy for ensuring that Departmental Elements test security controls periodically.

DOE Designation Order No. 00-28.00, section A.4.(d), states that “the CISO is responsible for assisting senior DOE officials concerning their responsibilities to provide information security for the information and information systems that support the operations and assets under their control, including through periodically testing and evaluating information security controls and techniques to ensure that they are effectively.”

DOE Office of Enterprise Assessment (EA) periodically assesses risk on behalf of the CIO to ensure the evaluations are unbiased. The CIO and CISO use the results of the assessment reports to further enhance site situational awareness, insight into the Department’s cyber risk posture, input into the Department Cyber Security Program, risk management policies, procedures, and strategy.

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 5:**

*Define the CISO’s role in Department policy for ensuring that the department has a process for planning, implementing, evaluating, and documenting remedial actions.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 currently defines the CISO’s role in Department policy for ensuring that the Department has a process for planning, implementing, evaluating, and documenting remedial actions.

DOE Designation Order No. 00-28.00, section A, 4.D, states that “The CISO is responsible for assisting senior DOE officials concerning their responsibilities to provide information security for the information and information systems that support the operations and assets under their control.” Although not explicitly stated, this responsibility includes ensuring the Department has a process for planning, implementing, evaluating, and documenting remedial actions.

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 6:**

*Define the CISO’s role in Department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the Department’s information systems in the event of a disruption.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 currently defines the CISO’s role in Department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the Department’s information systems in the event of a disruption.

FISMA 2014 section 3081, section 8, states that “The head of each agency shall be responsible for plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.” The Secretary of Energy delegates FISMA 2014 responsibilities to the CIO pursuant to DOE Redesignation Order No. 00-002.14. The CIO further designates these FISMA 2014 responsibilities and authority to the CISO through DOE Designation Order No. 00-28.00. DOE Designation Order No. 00-28.00, section A.1 states that “the CISO will carry out all FISMA responsibilities related to developing and maintaining a DOE-wide information security program.”

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 7:**

*Define the CISO’s role in Department policy for ensuring that personnel with significant security responsibilities receive appropriate training.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 and DOE O 205.1B currently defines the CISO’s role in Department policy for ensuring that all personnel with significant security responsibilities receive appropriate training.

Designation Order No. 00-28.00, paragraph 1.A.3 states that the CIO and its designee (CISO) has responsibilities for “training and overseeing personnel with significant information security responsibilities.”

In DOE O 205.1B, Section 1.d states that a core requirement of the DOE’s Risk Management Approach (RMA) is requiring a training, education, and awareness program” In addition, DOE O 205.1B, Sections 5.d and 5.e states that “The CIO and CISO have responsibility for maintaining the Department’s RMA.”

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 8:**

*Define the CISO’s role in department policy for oversight of contractor system security.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 currently defines the CISO’s role in Department policy for oversight of contractor system security.

FISMA section 3078 (a.1.A.ii) state that “the head of each agency shall be responsible for information systems used or operated by an agency or by a contractor of an agency, including



compliance to related policies, procedures, and standards.” The Secretary of Energy delegates FISMA 2014 responsibilities to the CIO pursuant to DOE Redesignation Order No. 00-002.14. The CIO further designates these FISMA 2014 responsibilities and authority to the CISO through DOE Designation Order No. 00-28.00. DOE Designation Order No. 00-28.00, section A states that “the CISO will carry out all FISMA responsibilities related to developing and maintaining a DOE-wide information security program.”

DOE Designation Order No. 00-28.00, section A.4.(d), states that “the CISO is responsible for assisting senior DOE officials concerning their responsibilities to provide information security for the information and information systems that support the operations and assets under their control, including through periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.”

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

**Recommendation 9:**

*Define the CISO’s role in Department policy in the periodic authorization of the department’s information systems.*

**Management Decision: Concur in Principle**

DOE Designation Order No. 00-28.00 and DOE O 205.1B currently define the CISO’s role in Department policy with respect to the periodic authorization of the Department’s information systems.

DOE Designation Order No. 00-28.00, section A.4.(d), states that “the CISO is responsible for assisting senior DOE officials concerning their responsibilities to provide information security for the information and information systems that support the operations and assets under their control, including through periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.”

DOE O 205.1B, Section 4.b Risk Management Process, describes the approach for ongoing monitoring and assessment of risk in information systems and determining acceptable risk tolerance levels. DOE O 205.1B, Section 4.b.(6), directs that, “Authorizing Officials are responsible and accountable for ensuring information systems under their purview are operated at an acceptable level of risk.” DOE O 205.1B, Section 6.e.(8) references alignment to Federal Information Process Standard (FIPS) 200 and the National Institute of Standards and Technology (NIST) 800 series, which are core standards required for assessing and authorizing information systems and must be defined in RMA implementation plans according to DOE O 205.1B, section 4.c.(1).

DOE is undertaking a review of DOE O 205.1B. During this review, the Department will consider the GAO recommendations.

**Estimated Completion Date: TBD**

# Appendix VI: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation  
Washington, DC 20201

JUL 28 2016

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

Dear Mr. Wilshusen:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Group Purchasing Organizations: Funding Structure has Potential to Inflate Medicare Costs*" (GAO-16-686).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

A handwritten signature in black ink that reads "Jim R. Esquea".

Jim R. Esquea  
Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED: GROUP PURCHASING ORGANIZATIONS: FUNDING STRUCTURE HAS POTENTIAL TO INFLATE MEDICARE COSTS (GAO-16-686)**

The U.S. Department of Health and Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

**Recommendation**

To ensure that the role of the CISO defined in department policy in accordance with FISMA 2014, we recommend that the Secretary of Health and Human Services take the following action:

- Define the CISO's role in department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the department's information systems in the event of a disruption.

**HHS Response**

HHS concurs with GAO's recommendation and anticipates that the updates to policy will be made in the next iteration of our Information Security and Privacy Policy in conjunction with anticipated revisions of National Institutes of Standards and Technology (NIST) 800-53, Revision 5.

# Appendix VII: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT  
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

JUL 22 2016

Mr. Nick Marinos  
Assistant Director, Information Technology  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to comment on the Government Accountability Office (GAO) draft report entitled, *Federal Chief Information Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority* (GAO-16-686). The U.S. Department of Housing and Urban Development (HUD) reviewed the draft report and has no comment.

The HUD Chief Information Security Officer (CISO) continues to strive for excellence in performing the CISO's key responsibilities. The CISO is committed to the established federal law and guidance and ensuring that HUD's security program requirements are properly documented and implemented.

If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 ([Janice.L.Ausby@hud.gov](mailto:Janice.L.Ausby@hud.gov)), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 ([Juanita.L.Toatley@hud.gov](mailto:Juanita.L.Toatley@hud.gov)).

Sincerely,

A handwritten signature in black ink, appearing to read "Rafael C. Diaz".

Rafael C. Diaz  
Chief Information Officer

# Appendix VIII: Comments from the Department of the Interior



## United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, D.C. 20240

JUL 28 2016

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

Dear Mr. Wilshusen:

Thank you for providing the Department of the Interior (Department) the opportunity to review and comment on the draft Government Accountability Office (GAO) Report entitled, *Federal Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority* (GAO-16-686). We appreciate GAO's government-wide review of the Chief Information Security Officer (CISO) authorities defined in Department policy in accordance with the Federal Information Security Modernization Act (FISMA) 2014.

The Department concurs with the four recommendations issued by GAO and is currently updating Department policy to ensure that the actions listed below are implemented.

1. Define the CISO's role in Department policy for ensuring that subordinate security plans are documented for the Department's information systems.
2. Define the CISO's role in Department policy for ensuring that plans and procedures are in place to ensure recovery and continued operation of the Department's information systems in the event of a disruption.
3. Define the CISO's role in Department policy for oversight of contractor system security.
4. Define the CISO's role in Department policy in the periodic authorization of the Department's information systems.

If you have any questions or need additional information, please contact me.

Sincerely,

Krysten J. Sarri  
Principal Deputy Assistant Secretary  
Policy, Management and Budget

# Appendix IX: Comments from the Department of Justice



U.S. Department of Justice

JUL 28 2016

Washington, D.C. 20530

Gregory Wilshusen  
Director  
Information Technology Security Issues  
United States Government Accountability Office  
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Justice (the Department or DOJ) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled "*Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*," (GAO-16-686), dated June 30, 2016. The Department concurs with the GAO's conclusions and recommendations.

Over the past 18 months, the Department has engaged in a comprehensive review and update of its cybersecurity policies and procedures to incorporate recent cybersecurity statutes and policies and to align with federal cybersecurity initiatives. The roles and responsibilities of the Department Chief Information Security Officer (CISO) are defined in the current DOJ Order 2640.2F Information Technology Security policy document, and amplified in the Department Cybersecurity Program Management Plan, as well as, through numerous cybersecurity program guidance and procedures documents. In practice, the CISO manages the Department's Cybersecurity Program, including the development and maintenance of policies, processes, and procedures, such as incident response, and review of system contingency plans. However, during the course of the review by the GAO team, it became clear that the descriptions of CISO roles and responsibilities in Order 2640.2F left some ambiguity around the responsibilities of the CISO in two areas: 1) ensuring risk-based IT security policies were established and maintained, and 2) that contingency plans and procedures were in place to ensure recovery and continued operations of the Department's information systems in the event of disruption. To address these two ambiguities, the Department has clarified the CISO responsibilities in the update of the cybersecurity program policy order, DOJ Order 0904 Cybersecurity Program, which is currently in final legal review and is expected to be released in August 2016. This action will address the following recommendations identified in Appendix II of the draft report.

**Recommendation:** That the Attorney General define the CISO's role in Department policy for ensuring that information security policies and procedures are developed and maintained.

**Response:** The description of the responsibilities of the CISO in the Department cybersecurity policy order will clearly state the responsibility to "establish, implement, and maintain cybersecurity policy and procedures."

Director Gregory Wilshusen

2

**Recommendation:** That the Attorney General define the CISO's role in Department policy for ensuring that plans and procedures are in place to ensure recovery and continued operations of the Department's information systems in the event of a disruption.

**Response:** The description of the responsibilities of the CISO in the Department cybersecurity policy order will clearly state the responsibility to "ensure that contingency plans are prepared."

Should you or your staff have any questions, please do not hesitate to contact Richard Theis, Assistant Director, Audit Liaison Group on 202-514-0469.

Sincerely,

*for Michael H. Allen*  
Lee J. Lofthus  
Assistant Attorney General for Administration  
Justice Management Division

# Appendix X: Comments from the Department of State



United States Department of State

Washington, DC 20520

JUL 27 2016

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

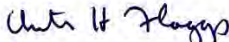
Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "FEDERAL CHIEF INFORMATION OFFICERS: Opportunities Exist to Improve Roles and Address Challenges to Authority." GAO Job Code 100105.

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

If you have any questions concerning this response, please contact Colleen Hinton, IT Policy Analyst, Office of Business Management and Planning, Bureau of Information Resource Management at (202) 634-0320.

Sincerely,

  
Christopher H. Flagg

Enclosure:  
As stated.

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



**Department of State Response to**

**GAO Draft Report: Federal Chief Information Security Officers  
Opportunities Exist to Improve Roles and Challenges to Authority**  
(GAO-16-686, GAO Code 100105)

The Department of State appreciates the opportunity to respond GAO draft Report, *Federal Chief Information Security Officers (CISO): Opportunities Exist to Improve Roles and Challenges to Authority*. There is one recommendation for the Department of State.

To ensure that the role of the CISO is defined in Department policy in accordance with FISMA 2014, GAO recommends that the Secretary of State take the following action: Define the CISO's role in department policy for ensuring that the department has procedures for incident detection, response, and reporting.

The Department concurs with the finding. The Department plans to correct the policy guidance contained in 5 FAM to show that the Diplomatic Security/Security Infrastructure/Cybersecurity/Monitoring and Incident Response Division (DS/SI/CS/MIRD) is the responsible entity.

Currently, the bureaus of Information Resource Management (IRM) and Diplomatic Security (DS) are continuing to work to further enhance and coordinate communications for the incident response process. Specifically, the Department has:

- Established the Joint Security Operations Center (JSOC).
- Established the Cyber Integrity Center (CIC).
- Deployed additional Senior Watch Officers (SWO's) at the Foreign Affairs Cybersecurity Center (FACC) to ensure the constant presence of supervisory personnel to direct and manage incident response program activities.

# Appendix XI: Comments from the Environmental Protection Agency



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

JUL 14 2016

Gregory Wilshusen  
Director, Information Technology Security Issues  
US Government Accountability Office  
441 G St. N.W.  
Washington, DC 20548

Dear Mr. Wilshusen:

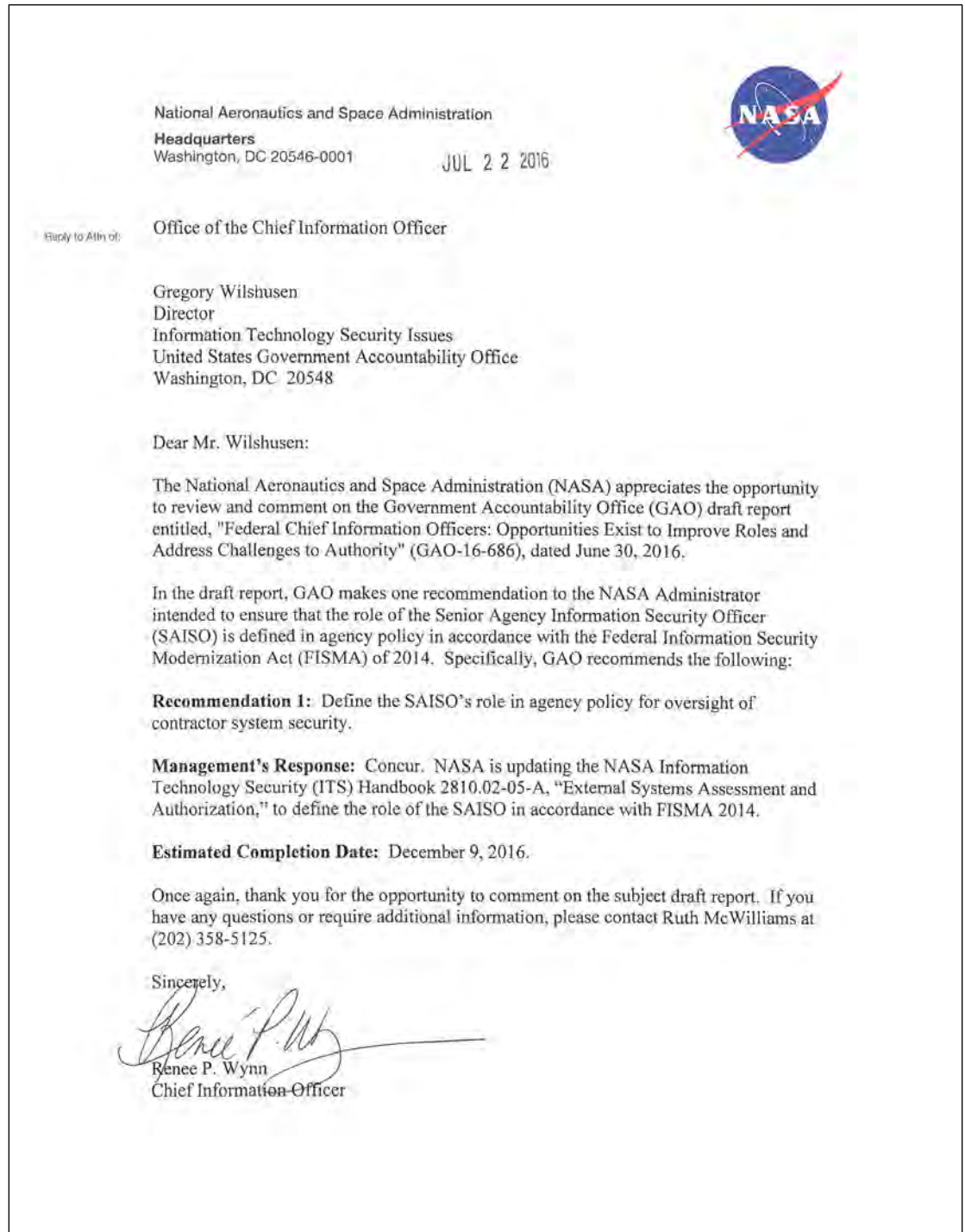
Thank you for providing the opportunity to review the U.S. Government Accountability Office's proposed report entitled *Federal Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, (GAO-16-686). I agree with the recommendations contained within the report. The identified recommendations will be implemented at the U.S. Environmental Protection Agency by July 29, 2016.

Sincerely,

A handwritten signature in black ink, appearing to read "Ann E. Dunkin".

Ann E. Dunkin  
Chief Information Officer

# Appendix XII: Comments from the National Aeronautics and Space Administration



# Appendix XIII: Comments from the U.S. Agency for International Development



**USAID**  
FROM THE AMERICAN PEOPLE

JUL 28 2016

Gregory Wilshusen  
Director  
Information Technology Security Issues  
U.S. Government Accountability Office  
44 G Street  
Washington, DC 20548

Re: FEDERAL CHIEF INFORMATION SECURITY OFFICERS: Opportunities Exist to Improve Roles and Address Challenges to Authority, GAO-16-686

Mr. Wilshusen:

I am pleased to provide the United States Agency for International Development's (USAID's) formal response to the Government Accountability Office (GAO) draft report entitled "*FEDERAL CHIEF INFORMATION SECURITY OFFICERS: Opportunities Exist to Improve Roles and Address Challenges to Authority*" (GAO-16-686).

This letter, together with the enclosed USAID comments, is provided for incorporation as an appendix to the final report. Thank you for the opportunity to respond to the GAO draft report and for the courtesies extended by your staff while conducting this GAO engagement.

Sincerely,

A handwritten signature in blue ink, appearing to read "Angelique M. Crumbly".

Angelique M. Crumbly  
Assistant Administrator  
Bureau for Management

Enclosure: a/s

- 2 -

**USAID COMMENTS ON GAO DRAFT REPORT**  
No. GAO-16-686

This report has one recommendation for USAID, on page 39 (Appendix II) of the draft report, as follows:

To ensure that the role of the CISO is defined in agency policy in accordance with FISMA 2014, we recommend that the Administrator of the U.S. Agency for International Development take the following action:

- Define the CISO's role in agency policy for oversight of contractor system security.

*Response:* USAID agrees with the recommendation. USAID/Office of the Administrator, in coordination with the Office of the Chief Information Officer, will update operational policy to define the CISO's role for oversight of contractor system security.

# Appendix XIV: Comments from the Social Security Administration



July 29, 2016

Mr. Gregory Wilshusen  
Director, Information Technology Security Issues  
United States Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review the draft report, "FEDERAL CHIEF INFORMATION SECURITY OFFICERS: Opportunities Exist to Improve Roles and Address Challenges to Authority" (GAO-16-686). We wish to share with you our activities in the area of strengthening the position of the Chief Information Security Officer (CISO) within our agency.

The Office of the Chief Information Officer (CIO) has delegated the role of the CISO to the Associate Commissioner of Information Security (OIS). OIS has made several changes in the last year to help strengthen the role of the CISO. Specifically, the CISO has moved the agency's Security Operation Center under OIS to be more efficient in reporting the agency's security infrastructure. OIS started the process of centralizing systems specialized security positions under the CISO by moving managerial responsibility for those individuals to the CISO's office. In addition, OIS started the process of authorizing applications that were developed and deployed outside the normal boundaries of our authorized systems. This includes developing security plans and provisional authorization for over 200 such applications in the last year. OIS is solely responsible for the oversight and execution of the System Authorization process for both Federal and Contractor systems. Finally, most recently, OIS completed the first authorization review of a cloud system that will host our modernized development environment.

While we still need more centralization of security responsibilities to support the *Federal Information Security Modernization Act* oversight requirements, we are confident that our CISO will continue to provide strong leadership over our information technology program.

If you have any questions, please contact me at (410) 965-0520. Your staff may contact Gary S. Hatcher, Senior Advisor for Records Management and Audit Liaison Staff, at (410) 965-0680.

Sincerely,

Frank Cristaudo  
Executive Counselor to the Commissioner

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

---

# Appendix XV: GAO Contact and Staff Acknowledgments

---

## GAO Contact

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

---

## Staff Acknowledgments

In addition to the individual named above, Nick Marinos (assistant director), William Cook (analyst in charge), Quintin Dorsey, Wayne Emilien, Paris Hawkins, Wil Holloway, Alan MacMullin, Lee McCracken, David Plocher, Kelly Rubin, Edward Varty, Brian Vasquez, and Adam Vodraska made significant contributions to this report.

---

---

## GAO's Mission

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

---

## Obtaining Copies of GAO Reports and Testimony

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

---

## Order by Phone

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

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

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

---

## Connect with GAO

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

---

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

Contact:

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

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

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

---

## Congressional Relations

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

---

## Public Affairs

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

---

## Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, [spel@gao.gov](mailto:spel@gao.gov), (202) 512-4707, U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548



Please Print on Recycled Paper.