United States Government Accountability Office

Report to Congressional Committees

August 2018

# FEDERAL CHIEF INFORMATION OFFICERS

# Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities

Accessible Version

GAO-18-93

**August 2018**

# FEDERAL CHIEF INFORMATION OFFICERS

## Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities

GAO

# Highlights

Highlights of GAO-18-93, a report to congressional committees

## Why GAO Did This Study

Agencies plan to spend more than $96 billion on IT in fiscal year 2018; however, they continue to face longstanding challenges in doing so. Congress established the CIO position to serve as an agency focal point for IT to address these challenges.

Recognizing the importance of the CIO position to successful IT management, GAO was asked to conduct a government-wide review of CIO responsibilities. GAO's objectives were to determine (1) the extent to which agencies have addressed the role of the CIO in accordance with federal laws and guidance, and (2) major factors that have enabled and challenged agency CIOs in fulfilling their responsibilities to carry out federal laws and guidance. To do so, GAO reviewed laws and OMB guidance to identify key IT management responsibilities of federal agency CIOs and then compared them to policies of the 24 Chief Financial Officers Act agencies. GAO also administered a survey to 24 CIOs and interviewed current CIOs, as well as OMB officials.

## What GAO Recommends

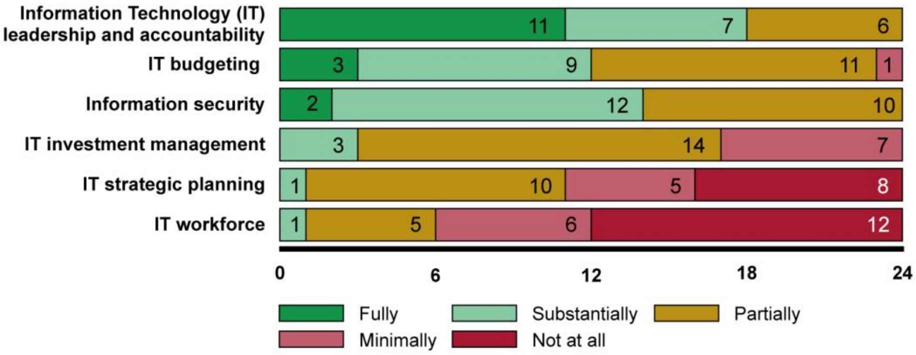
GAO is making three recommendations to OMB and one recommendation to each of the 24 federal agencies to improve the effectiveness of CIOs' implementation of their responsibilities for each of the six IT management areas. (See the next page for additional information on these recommendations).

View GAO-18-93. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov or Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

## What GAO Found

None of the 24 agencies have policies that fully addressed the role of their Chief Information Officers (CIO) consistent with federal laws and guidance. In addition, the majority of the agencies did not fully address the role of their CIOs for any of the six key areas that GAO identified (see figure 1).

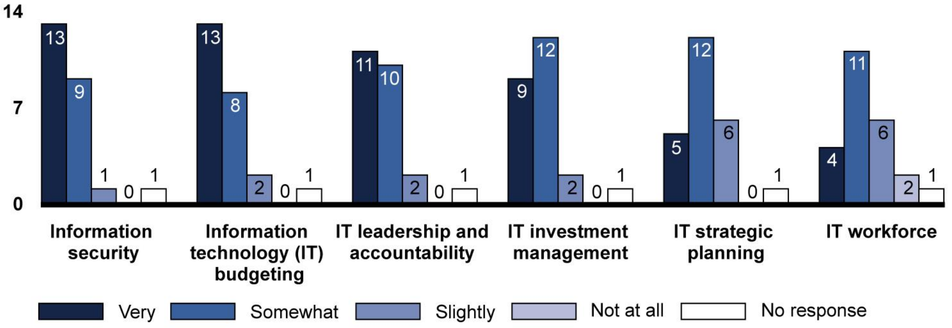
**Figure 1: Extent to Which 24 Agencies' Policies Addressed the Role of Their Chief Information Officers, Presented from Most Addressed to Least Addressed Area**



Source: GAO analysis of agency IT management policies. | GAO-18-93

Among other things, officials from most agencies stated that their CIOs are implementing the responsibilities even when not required in policy. Nevertheless, the 24 selected CIOs acknowledged in their responses to GAO's survey that they were not always very effective in implementing the six information technology (IT) management areas (see figure 2). Until agencies fully address the role of CIOs in their policies, agencies will be limited in addressing longstanding IT management challenges.

**Figure 2: Extent to Which Chief Information Officers Reported Effective Implementation of Six Responsibility Areas, Presented from Most Effective to Least Effective Area**



Source: Chief information officer responses to GAO survey. | GAO-18-93

Shortcomings in agencies' policies are partially attributable to two weaknesses in the Office of Management and Budget's (OMB) guidance. First, the guidance does not comprehensively address all CIO responsibilities, such as those relating to assessing the extent to which personnel meet IT management knowledge and skill requirements and ensuring that personnel are held accountable for complying with the information security program. Correspondingly, the majority of

GAO is making the following three recommendations to OMB:

1. Issue guidance that addresses the responsibilities that are not included in existing OMB guidance—in particular those relating to IT workforce.
2. Update existing guidance to clearly explain how agencies are to address the role of CIOs to comply with the statutory requirements for CIOs to have a significant role in (1) budgeting decisions and (2) the management, governance, and oversight processes related to IT.
3. Define the authority that CIOs are to have when agencies report on CIO authority over IT spending.

GAO is also making a recommendation to each of the 24 federal agencies to address weaknesses related to the six key areas of CIO responsibility.

Fourteen agencies agreed with GAO's recommendations, and five agencies had no comments on the recommendations.

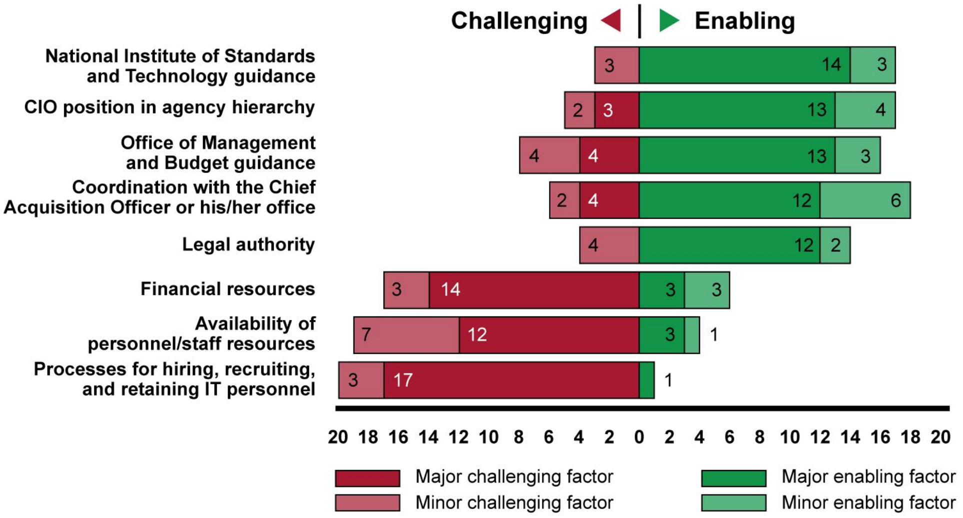
In addition, five agencies (including OMB) partially agreed with GAO's recommendations and one agency disagreed. In particular, five of these agencies did not agree with select assessments of select CIO responsibilities. GAO subsequently updated two assessments but believes the other assessments and related recommendations are warranted, as discussed in the report. The remaining agency—OMB—partially agreed with GAO's recommendation to issue guidance for responsibilities that are not included in existing OMB guidance. GAO continues to believe that this recommendation is warranted, as discussed in the report.

Moreover, after GAO provided the draft report to OMB for comment, the President signed an executive order that, among other things, clarified the role that CIOs are to have in the management, governance, and oversight processes related to IT. The executive order is responsive to GAO's related recommendation. GAO will continue to monitor agencies' implementation of the executive order.

the agencies' policies did not fully address nearly all of the responsibilities not included in OMB guidance. Second, OMB guidance does not ensure that CIOs have a significant role in (1) IT planning, programming, and budgeting decisions and (2) execution decisions and the management, governance, and oversight processes related to IT. In the absence of comprehensive guidance, CIOs will not be positioned to effectively acquire, maintain, and secure their IT systems.

In GAO's survey, the 24 agency CIOs identified a number of factors that enabled and challenged their ability to effectively manage IT. In particular, five factors were identified by at least half of the 24 CIOs as major enablers and three factors were identified by at least half of the CIOs as major challenges. (see figure 3). Further, GAO noted that agencies continue to lack consistent leadership in the CIO position.

**Figure 3: Factors Commonly Identified as Enabling and Challenging Chief Information Officers (CIO) to Effectively Manage Information Technology (IT), Presented from Most Enabling to Least Enabling Factor**



Source: Chief information officer responses to GAO survey. | GAO-18-93

Although OMB has issued guidance aimed at addressing the three factors that were identified by at least half of the CIOs as major challenges, the guidance does not fully address those challenges. In particular, with respect to the challenges relating to IT personnel, OMB's guidance does not address key CIO responsibilities, as previously noted. Further, regarding the financial resources challenge, OMB recently required agencies to provide data on CIO authority over IT spending; however, OMB's guidance does not provide a complete definition of the authority. In the absence of this guidance from OMB, agencies have created varying definitions of CIO authority. Until OMB updates its guidance to include a complete definition of the authority that CIOs are to have over IT spending, it will be difficult for OMB to identify any deficiencies in this area and help agencies to make any needed improvements.

# Contents

Tables

Figures

**Abbreviations**

| | |
|---|---|
| Agriculture | Department of Agriculture |
| CAO | chief acquisition officer |
| CIO | chief information officer |
| CISO | chief information security officer |
| Commerce | Department of Commerce |
| Defense | Department of Defense |
| DHS | Department of Homeland Security |
| Education | Department of Education |
| Energy | Department of Energy |
| 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 |
| GSA | General Services Administration |
| HHS | Department of Health and Human Services |
| HUD | Department of Housing and Urban Development |
| IRM | information resources management |
| IT | information technology |
| Interior | Department of the Interior |
| Justice | Department of Justice |
| Labor | Department of Labor |
| MGT | Modernizing Government Technology Act |
| NASA | National Aeronautics and Space Administration |
| NIST | National Institute of Standards and Technology |
| NRC | Nuclear Regulatory Commission |
| NSF | National Science Foundation |
| OIRA | Office of Information and Regulatory Affairs |
| OMB | Office of Management and Budget |
| OPM | Office of Personnel Management |
| SBA | Small Business Administration |
| SSA | Social Security Administration |
| State | Department of State |
| Transportation | Department of Transportation |

| | |
|---|---|
| Treasury | Department of the Treasury |
| USAID | U.S. Agency for International Development |
| VA | Department of Veterans Affairs |

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

August 2, 2018

Congressional Committees

Information systems are critical to the health, economy, and security of the nation. To develop and maintain these systems, in fiscal year 2018, federal agencies plan to spend more than $96 billion on information technology (IT). Although the government makes these substantial annual investments, it faces longstanding problems in its management of IT. Our most recent high-risk series update continues to identify the management of IT acquisitions and operations and information security as government-wide challenges.[1]

Over the years, Congress has enacted various laws in an attempt to improve the government's management of IT. For example, the Clinger-Cohen Act of 1996 required agency heads to designate Chief Information Officers (CIO) to lead reforms that would help control system development risks, better manage technology spending, and achieve measurable improvements in agency performance.[2] In addition, the Federal Information Security Management Act of 2002[3] (FISMA 2002) and its successor, the Federal Information Security Modernization Act of 2014 (FISMA 2014),[4] make CIOs responsible for ensuring that agencies develop, document, and implement information security programs. Further, federal IT acquisition reform legislation (commonly referred to as the Federal Information Technology Acquisition Reform Act, or FITARA), which was enacted in December 2014, strengthened the role of covered agency CIOs in managing IT.[5]

[1] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[2] 40 U.S.C. §§ 11312 and 11313.

[3] Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[4] Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).

[5] Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438 (Dec. 19, 2014).

We also have long been proponents of having strong agency CIOs in place to lead federal agencies' management of IT. In July 2004 and September 2011, we reported on federal agency CIOs, including their responsibilities, tenure, and challenges.[6] Further, in September 2016 the Comptroller General convened a forum with current and past CIOs, which explored challenges and opportunities for CIOs to improve federal IT acquisitions and operations.[7]

Recognizing the continued importance of the CIO position in achieving better results through IT management, you asked us to conduct a government-wide review of CIO responsibilities. Our specific objectives were to (1) determine the extent to which agencies have addressed the role of the CIO in accordance with federal laws and guidance, and (2) describe major factors that have enabled and challenged agency CIOs in fulfilling their responsibilities to carry out federal laws and guidance.

To address the first objective, we created an evaluation framework and assessed the management policies of selected agencies against this framework. To create the evaluation framework, we reviewed relevant laws—such as the Clinger-Cohen Act of 1996, FISMA 2014, and FITARA—to identify key IT management responsibilities of federal CIOs.[8] After completing our review of these laws, we reviewed key requirements discussed in the Office of Management and Budget's (OMB) guidance on agency CIO IT management and information security responsibilities, such as *Management and Oversight of Federal Information Technology, Memorandum M-15-14*.[9]

Based on our reviews of the laws and guidance, we identified 35 key CIO IT management responsibilities and categorized them in six management

[6] GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, GAO-11-634 (Washington, D.C.: Sept. 15, 2011); and *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: Jul. 21, 2004).

[7] GAO, *Information Technology: Opportunities for Improving Acquisitions and Operations*, GAO-17-251SP (Washington, D.C.: Apr. 11, 2017).

[8] We did not review the following CIO responsibilities relating to information management: information collection/paperwork reduction, information dissemination, information disclosure, statistical policy and coordination, records management, and privacy.

[9] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

areas.[10] We then compared the responsibilities in this framework to IT management policies from each of the 24 departments and agencies covered by the Chief Financial Officers Act.[11]

In addition, we administered a survey to the CIOs of each of the 24 agencies from December 2016 to February 2017.[12] In the survey, we asked the CIOs to identify how effective they have been in carrying out the key IT management responsibilities since December 2014, when FITARA was enacted. We then interviewed 22 CIOs and 1 Deputy CIO[13] to obtain additional insights on their survey responses.[14] We also interviewed officials from OMB's Office of E-Government and Information Technology to obtain information about the agency's guidance on IT management responsibilities of CIOs.

To address the second objective, we asked the CIOs in our survey to describe the extent to which certain factors have enabled and challenged their ability to effectively carry out the key IT management responsibilities since December 2014, when FITARA was enacted. Specifically, in the survey, we identified 25 potential factors that could enable or challenge the CIOs' ability to effectively manage IT.[15] We asked the CIOs to rate whether each factor was a minor enabler, major enabler, minor challenge, major challenge, or neither enabling nor challenging. We then

[10] The six areas are: IT leadership and accountability, IT strategic planning, IT workforce, IT budgeting, IT investment management, and information security.

[11] 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.

[12] The survey for the Department of Defense was completed by the Deputy CIO.

[13] The Department of Homeland Security made the Deputy CIO available for an interview, in lieu of the CIO.

[14] The CIO of the remaining agency—the Department of Defense—declined to meet with us.

[15] To develop the list of 25 factors, we reviewed our prior work on enabling and challenging factors for Chief Information Security Officers and discussed the list with internal subject matter experts for their relevance to the CIOs. We also pretested the survey with officials at five agencies to ensure that the list of factors was complete.

summarized the CIOs' survey responses by focusing on factors that were identified by CIOs as major enablers and major challenges. We also met with representatives from OMB's Office of E-Government and Information Technology to discuss the office's efforts to address factors that have challenged the CIOs' ability to effectively carry out the key IT management responsibilities. In addition, we collected and analyzed information on the tenure of the 24 agencies' current and former CIOs. Additional details on our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from August 2016 to August 2018 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.

# Background

Congress has long recognized that IT has the potential to enable federal agencies to accomplish their missions more quickly, effectively, and economically. However, fully exploiting this potential has presented longstanding challenges to agencies, and the federal government's management of IT has often produced mixed results. The CIO position was established by Congress to serve as a focal point for IT and related information management functions within an agency to help address these challenges.

## Congress, OMB, and the Current Administration Have Established CIO Roles and Responsibilities

Over the past 38 years, various laws were enacted that outlined roles and responsibilities for agency CIOs in an attempt to improve the government's performance in IT and related information management functions. For example:

- In 1980, the Paperwork Reduction Act[16] required that each agency head designate a senior official who would directly report to the

[16] Pub. L. No. 96-511 (Dec. 11, 1980).

head to be responsible for the management of the agency's information activities and information systems. In 1995, the law was amended to place the management of IT under the umbrella of information resources management (IRM)[17] and required agencies to develop processes to select, control, and evaluate the results of major information systems initiatives.[18]

- In 1996, the Clinger-Cohen Act supplemented provisions of the Paperwork Reduction Act with detailed requirements for IT strategic planning, budgeting, and investment management.[19] The act also established the agency CIO position by renaming the senior IRM officials "chief information officers" and specifying additional responsibilities for them.[20] For example, the act calls for CIOs to assess agency IT workforce needs and to develop strategies and plans for meeting those needs.[21]
- To address information security challenges in the federal government, Congress enacted FISMA 2002, and its successor, FISMA 2014. These laws require agencies to develop, document, and implement a program to provide security for the information and information systems that support the operations and assets of the agency. These laws also direct agency heads to delegate to agency CIOs authority to ensure compliance with the law. In turn, CIOs are required to designate a senior agency information security officer to carry out these responsibilities. This official is generally referred to as a chief information security officer (CISO).
- In December 2014, FITARA was enacted to, among other things, further strengthen the authority of agency CIOs. For example, the law requires covered agencies[22] to ensure that their CIOs have a

[17] Pub. L. 104-13 (May 22, 1995); 44 US.C. § 3501, et. seq. IRM is the process of managing information resources to accomplish agency missions and to improve agency performance. 44 U.S.C. § 3502(7).

[18] 44 U.S.C. § 3506(h)(5).

[19] 40 U.S.C. §§ 11312 and 11313.

[20] 40 U.S.C. § 11315 and 44 U.S.C. § 3506(a). The Clinger-Cohen Act requirement that agency CIOs have IRM as their primary duty applies to the 24 major departments and agencies listed in 31 U.S.C. § 901(b). The E-Government Act of 2002 reiterated agency responsibility for information resources management. P.L. 107-347 (Dec. 17, 2002).

[21] 40 U.S.C § 11315(c)(3).

[22] The provisions apply to the agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b), but has limited application to the Department of Defense.

significant role in the decision process for budgeting, as well as the management, governance, and oversight processes related to IT. In addition, FITARA requires covered agency CIOs to (1) review and approve contracts for IT and (2) approve the appointment of other bureau officials with the title of CIO.[23]

Further, these and other laws assign two offices within OMB—the Office of Information and Regulatory Affairs (OIRA) and the Office of E-Government and Information Technology—key roles in helping agencies effectively manage IT.

- **OIRA.** The Paperwork Reduction Act of 1980 established OIRA within OMB and gave the office responsibility for oversight of federal IT management (then termed automatic data processing and telecommunications functions).[24] The 1995 amendments to the Paperwork Reduction Act continued these responsibilities, therein referred to as IT management. The 1996 Clinger-Cohen Act further required OMB to strengthen federal IT management through the use of capital planning and investment control, and performance management.[25]
- **Office of E-Government and Information Technology.** In 2002, Congress enacted the E-Government Act to address the challenges of managing federal government programs and services in the age of the Internet. To assist in this effort, the act established the Office of Electronic Government within OMB (now called the Office of E-Government and Information Technology). This office is headed by the Federal CIO[26] and, in coordination

[23] For purposes of this report, the term "bureau" refers to a principal subordinate organizational unit of an agency (e.g., component, service, or operating division). This term is used by OMB in its guidance.

[24] The Paperwork Reduction Act of 1980 also gave the OIRA responsibilities for the oversight of general information policy; reduction of paperwork burden; federal statistical policy; records management; and information privacy, disclosure, and security. These responsibilities were continued in the Paperwork Reduction Act of 1995.

[25] 40 U.S.C. §§ 11302 & 11303.

[26] The Federal CIO is the presidential designation for the Administrator of the OMB Office of E-Government and Information Technology, which is the head of the office under the E-Government Act.

with OIRA, is responsible for overseeing the implementation of IT management responsibilities.[27]

Under these authorities, OMB has issued guidance to agencies on many IT management areas. For example, in the last 3 years, OMB has issued:

- implementation guidance for FITARA and related IT management practices,[28]
- annual guidance on federal information security and privacy management requirements,[29]
- revisions to *Circular No. A-130, Managing Information as a Strategic Resource*,[30] and
- implementation guidance[31] for the Modernizing Government Technology (MGT) Act.[32]

Most recently, on May 15, 2018, the President signed Executive Order 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*. Among other things, this executive order is intended to better position agencies to modernize their IT systems, execute IT programs more efficiently, and reduce cybersecurity risks.[33] The order pertains to 22 of

[27] Under the Paperwork Reduction Act, OIRA continues to be responsible for overseeing federal IT management and information management functions. 44 U.S.C. §§ 3503 & 3504. Under the E-Government Act of 2002, the Office of E-Government and Information Technology and OIRA are to work together in setting strategic direction and overseeing the implementation of e-government under the act and relevant laws, including the Paperwork Reduction Act and the Clinger-Cohen Act. 44 U.S.C. § 3602(d)&(e).

[28] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[29] See OMB, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*, M-18-02 (Oct. 16, 2017).

[30] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 28, 2016).

[31] OMB, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

[32] MGT provisions of the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G (Dec. 12, 2017). The MGT Act authorizes agencies to establish working capital funds for use in transitioning from legacy IT systems, as well as for addressing evolving threats to information security. The law creates a technology modernization fund within the Department of the Treasury, from which agencies can draw on to help retire and replace legacy systems as well as acquire or develop systems.

[33] Exec. Order No. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*; 83 Fed. Reg. 23345 (May 15, 2018).

the 24 Chief Financial Officer Act agencies; the Department of Defense (Defense) and the Nuclear Regulatory Commission (NRC) are exempt.

For the covered agencies, the executive order is intended to strengthen the role of agency CIOs by, among other things, requiring them to (1) report directly to their agency head; (2) to serve as their agency head's primary IT strategic advisor; and (3) have a significant role in all management, governance, and oversight processes related to IT. In addition, one of the cybersecurity requirements directs agencies to ensure that the CIO works closely with an integrated team of senior executives, including those with expertise in IT, security, and privacy, to implement appropriate risk management measures.

## GAO and Others Have Reported on CIOs' Roles and Responsibilities

We and others have previously reported on CIOs' roles and responsibilities, including steps agencies could take to strengthen the roles of their CIOs.

- In reporting on CIOs' roles and responsibilities in July 2004, for example, we noted that not all CIOs exercised all responsibilities required by statute or that were critical to effective IT management.[34] In addition, we examined the tenure of these officials, noting that CIOs and former agency IT executives believed it was necessary for a CIO to stay in office for 3 to 5 years to be effective. However, at the time of our review, the median tenure of permanent CIOs whose time in office had been completed was about 2 years.

We also reported on major challenges that the CIOs said they faced in their duties. In this regard, the vast majority of them reported a number of substantial challenges related to IT workforce (e.g., recruiting and retention) and the development and implementation of agency IT budgets. We stressed that effectively tackling these reported challenges could improve the likelihood of a CIO's success. We suggested that Congress consider whether existing statutory requirements related to CIO responsibilities reflected the most effective assignment of IT management responsibilities and reporting relationships.

[34] GAO-04-823.

- Based on a follow-up review of CIOs’ roles and responsibilities, in September 2011, we reported that CIOs did not consistently have responsibility for 13 major areas of IT and information management as defined by law or deemed critical to effective IT management. In addition, we found that just over half of the CIOs reported directly to the heads of their respective agencies and that the tenure of the CIO position remained at about 2 years.[35] (See appendix II for updated information on the tenure of CIOs between 2004 and 2017 for each of the agencies in this review.)

Further, we noted that more consistent implementation of CIOs’ authority could enhance their effectiveness. While OMB had taken steps to increase CIOs’ effectiveness, it had not established measures of accountability to ensure that responsibilities were fully implemented. Accordingly, we recommended that OMB update its guidance to ensure that CIOs’ responsibilities were fully implemented and require agencies to establish internal processes for documenting lessons learned. OMB officials generally agreed with our recommendations and, as previously mentioned, issued guidance in June 2015 describing actions that agencies are to take in order to provide CIOs with the authority called for by FITARA and select provisions the Clinger-Cohen Act.[36]

- In August 2016, we reported on 24 agencies’ implementation of CISO authorities.[37] In particular, the 24 CISOs that we surveyed identified factors that limited their abilities to carry out their responsibilities, including 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.
- We also found that, although OMB had a statutory responsibility under FISMA 2014 to provide guidance on information security in federal agencies, it had not issued such guidance addressing how agencies should ensure that officials carry out their responsibilities and how personnel are held accountable for complying with the agency-wide information security programs. We recommended, among other things, that OMB issue guidance for clarifying CISOs’

[35] GAO-11-634.

[36] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[37] GAO, *Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority*, GAO-16-686 (Washington, D.C.: Aug. 26, 2016).

roles in light of identified challenges. OMB partially concurred with the recommendation, but did not intend to directly issue guidance as recommended.

- In September 2016, the Comptroller General convened a forum regarding improvements needed for IT acquisitions and operations.[38] Given the importance of CIOs to the management of the government's IT portfolio, the forum had a special focus on how CIOs could help improve delivery and operations. Forum participants, including 13 current and former federal agency CIOs, members of Congress, and private sector IT executives, identified key actions related to seven topics: (1) strengthening FITARA, (2) improving CIO authorities, (3) budget formulation, (4) governance, (5) workforce, (6) operations, and (7) transition planning. Of note, participants cited actions that could help improve CIO authorities, such as implementing collaborative governance and evolving the role of the CIO to enable change.
- In January 2017, the Federal CIO Council[39] reported on the state of federal IT.[40] The council pointed out that CIOs continue to face a host of challenges ranging from budget shortfalls, large legacy IT portfolios, and ever-increasing cybersecurity threats, to difficulties in attracting and retaining top-tier talent in a highly competitive field. The council made a number of recommendations to address these challenges, including to clarify the role of the CIOs at the government-wide and agency levels, and to establish central funding for shared services and infrastructure modernization.

## Agencies Have Not Fully Addressed the Role of Their CIOs in Accordance with Federal Laws and Guidance

Federal laws and guidance assign to agency CIOs 35 key responsibilities for effectively managing IT, which should be documented in agencies'

[38] GAO-17-251SP.

[39] The Federal CIO Council is the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources.

[40] CIO Council, *State of Federal Information Technology* (January 2017).

policies. These responsibilities are in six areas: leadership and accountability, strategic planning, workforce, budgeting, investment management, and information security. Table 1 identifies the 35 responsibilities and six areas. (Appendix I identifies the legal authority for each responsibility.)

Table 1: Summary of Key Chief Information Officer (CIO) Responsibilities

| Responsibility |
|---|
| **Information technology (IT) leadership and accountability** – *CIOs are responsible and accountable for the effective implementation of IT management responsibilities.* |
| Report directly to the agency head or that official's deputy.[a] |
| Assume responsibility and accountability for IT investments. |
| Approve the selection of bureau CIOs. |
| Provide input into bureau CIO performance evaluations. |
| Designate a senior agency information security officer. |
| **IT strategic planning** – *CIOs are responsible for strategic planning for all IT management functions.* |
| Establish goals for improving agency operations through IT. |
| Measure how well IT supports agency programs. |
| Prepare an annual report on the progress in achieving the goals. |
| Benchmark agency processes against private and public sector performance. |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments. |
| **IT workforce** – *CIOs are responsible for assessing agency IT workforce needs and developing strategies and plans for meeting those needs.* |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills. |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements. |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies. |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities. |
| **IT budgeting** – C*IOs are responsible for the processes for all annual and multi-year IT planning, programming, and budgeting decisions.* |
| Have a significant role in IT planning, programming, and budgeting decisions. |
| Ensure that the agency implements a process for selecting IT investments. |
| Review and approve the IT budget request. |
| Review and approve funding reprogramming requests (i.e., shifting funds within an appropriation fund or account). |
| **IT investment management** – *CIOs are responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources*. |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT. |
| Improve the management of the agency's IT through portfolio review (PortfolioStat). |
| Ensure that the agency implements a process for controlling and evaluating IT investments. |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings). |
| Review high-risk IT investments (TechStat sessions). |
| Certify that investments are adequately implementing incremental development consistent with Office of Management and Budget (OMB) capital planning guidance. |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation. |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented. |

| Responsibility |
|---|
| Review and approve IT contracts, acquisition plans, or strategies.[b] |
| Maintain an inventory of data centers. |
| Maintain a strategy to consolidate and optimize data centers. |
| **Information security** – *CIOs are responsible for establishing, implementing, and ensuring compliance with an agency-wide information security program.* |
| Develop and maintain an agency-wide information security program. |
| Develop and maintain information security policies, procedures, and control techniques. |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities. |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques. |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program. |
| Report annually to the agency head on the effectiveness of the agency information security program. |

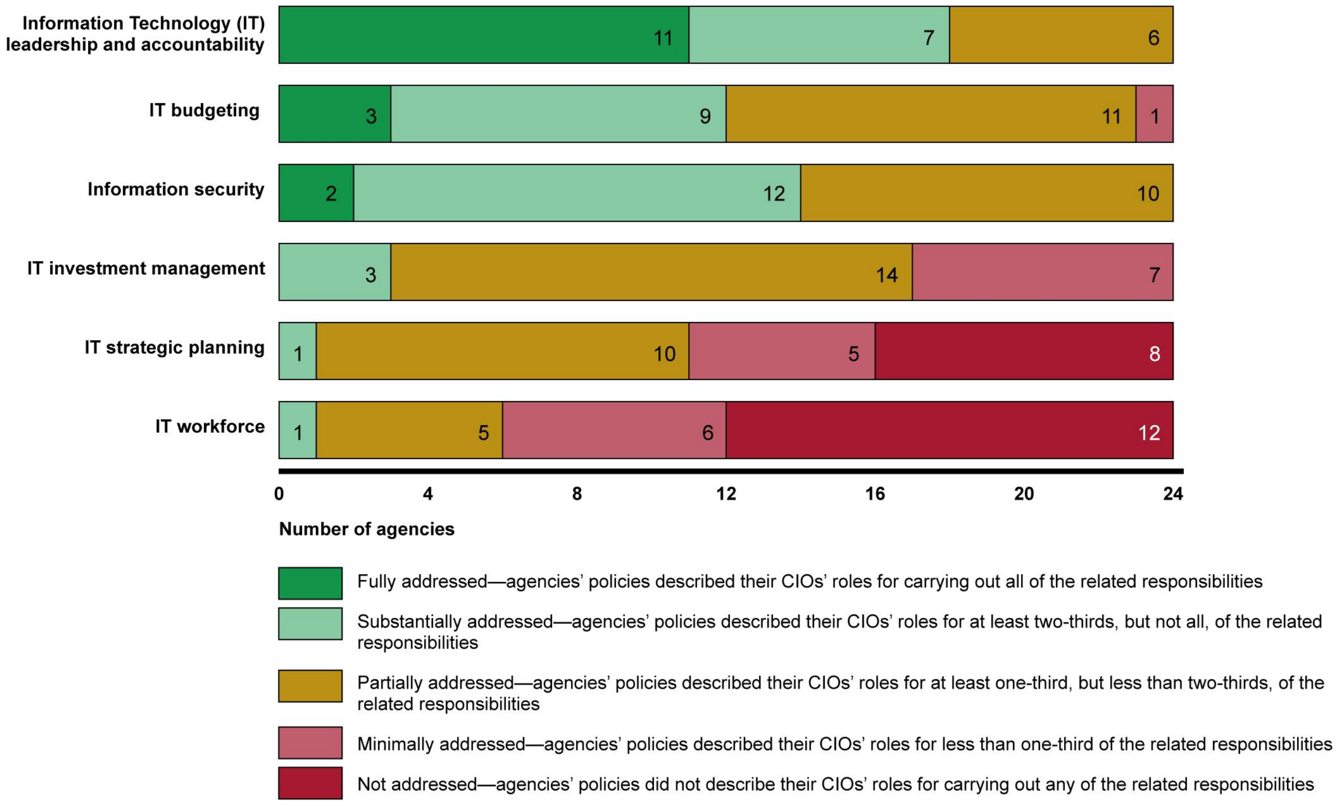
Source: GAO analysis of federal legislation and guidance. | GAO-18-93

[a] The law requires the CIO to report directly to the agency head, and OMB's implementing guidance states that CIOs may report to the head of the agency (e.g., secretary) or that official's deputy (e.g., deputy secretary) who acts on behalf of the agency's overall leader.

[b] The law requires CIOs to review and approve IT contracts, and OMB's implementing guidance states that CIOs may review and approve IT acquisition strategies and plans, rather than individual IT contracts.

None of the 24 selected agencies' IT management policies have fully addressed the role of their CIOs consistent with federal laws and guidance. In this regard, a majority of the agencies fully or substantially addressed the role of their CIOs for the area of leadership and accountability. In addition, a majority of the agencies substantially or partially addressed the role of their CIOs for two areas: IT budgeting and information security. However, most agencies partially or minimally addressed the role of their CIOs for two areas: investment management and strategic planning. Further, the majority of the agencies minimally addressed or did not address the role of their CIOs for the remaining area: IT workforce. Figure 1 depicts the extent to which the 24 agencies addressed the role of their CIOs for the six areas. (Also see appendix III, which provides additional details on our assessment of the extent to which the policies of each agency addressed each of the six areas and the key 35 responsibilities that comprise them.)

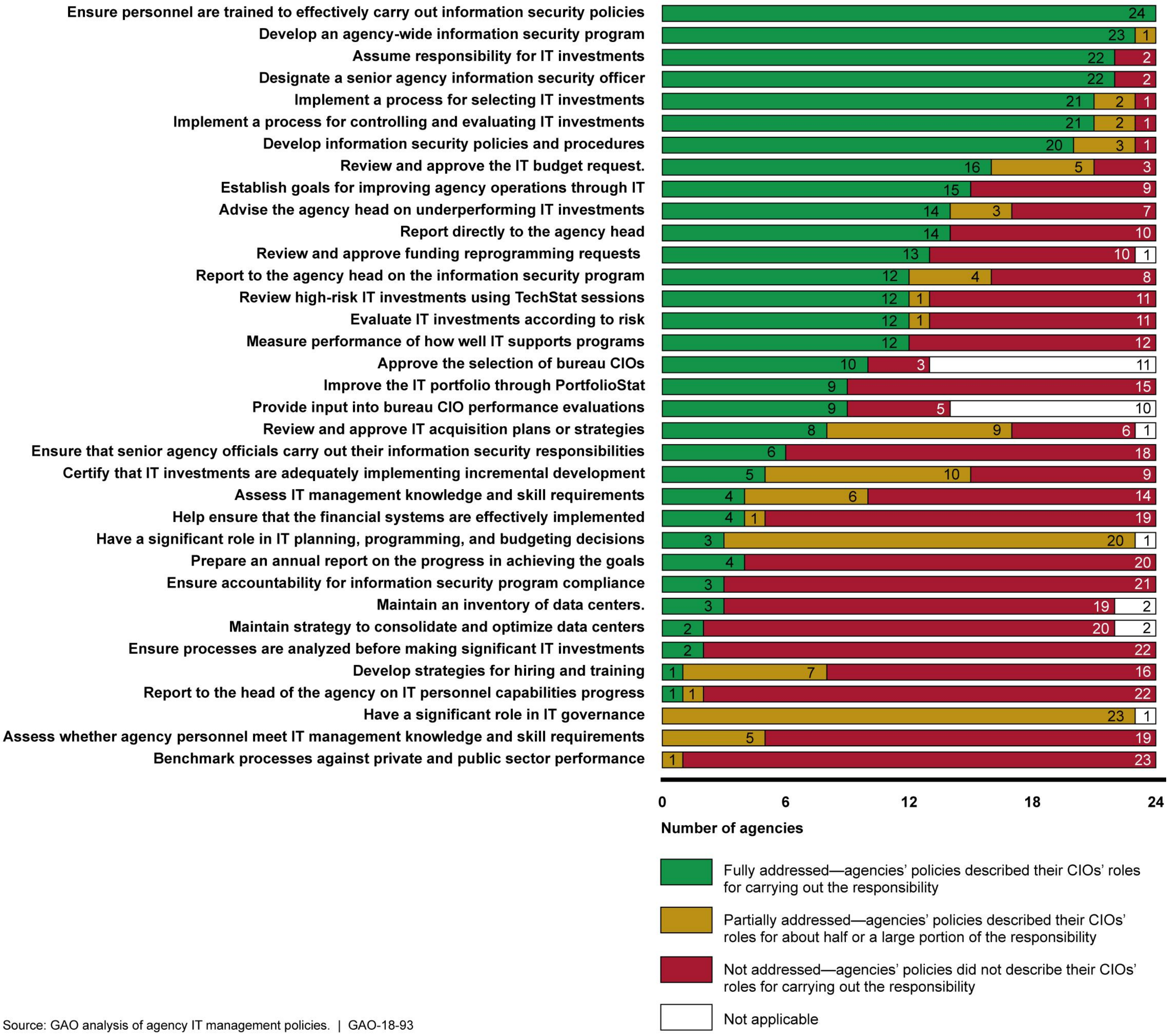
**Figure 1: Extent to Which 24 Selected Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO), Presented from Most Addressed to Least Addressed Area**



Source: GAO analysis of agency IT management policies. | GAO-18-93

Within the six areas, none of the 24 agencies fully addressed all 35 responsibilities in their policies. Figure 2 summarizes the extent to which the agencies addressed each of the responsibilities. (Appendix IV contains more detailed information regarding the extent to which the policies of the 24 agencies addressed the 35 responsibilities.)

### Figure 2: Extent to Which 24 Selected Agencies' Policies Addressed the Role of Their Chief Information Officers (CIOs), Presented from Most Addressed to Least Addressed Responsibility



Source: GAO analysis of agency IT management policies. | GAO-18-93

As shown in figure 2, only 18 of the 35 responsibilities were fully addressed in the policies of half or more of the applicable agencies.[41] For example:

- **Develop and maintain an information security program.** The policies for 23 agencies addressed the role of their CIOs for this responsibility. For example, the Department of Agriculture's (Agriculture) regulation on security assessment and authorization makes the CIO responsible for developing and maintaining an agency-wide information security program.

  However, the policy of the 1 remaining agency—the National Aeronautics and Space Administration (NASA)—partially addressed this responsibility. Although NASA established a policy requiring the CIO to develop and maintain an information security program, the Assistant Administrator for the Office of Protective Services (rather than the CIO) was assigned responsibility for developing such a program for classified national security systems.

- **Select IT investments.** The policies of 21 agencies fully addressed the role of their CIOs in the selection of IT investments. For example, the Department of Health and Human Services' (HHS) IT Capital Planning and Investment Control policy states that its CIO is responsible for establishing an IT investment selection process and ensuring that all operating divisions comply with that process.

  However, the policies of 2 agencies—the Departments of Energy (Energy) and Justice (Justice)—partially addressed this responsibility. Specifically, the policies of these agencies required the CIOs to implement processes for selecting some, but not all, IT investments. One other agency—the Department of the Treasury (Treasury)—did not address this responsibility.

- **Report directly to the agency head or that official's deputy.** Fourteen agencies' policies fully addressed the role of their CIOs

[41] Five of the 35 responsibilities do not apply to the Department of Defense because it was exempted from these responsibilities under FITARA. Additionally, 2 responsibilities—approve the selection of bureau CIOs and provide input into bureau CIO performance evaluations—do not apply to 10 agencies without bureau CIOs. The 10 agencies without bureau CIOs are the: Departments of State and Veterans Affairs, as well as the Environmental Protection Agency, General Services Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

for this responsibility.[42] For example, according to Defense's policy on CIO responsibilities, its CIO is to report directly to the Secretary of Defense. As another example, the Department of Veterans Affairs' (VA) policies state that the Assistant Secretary for Information and Technology, who serves as the CIO for the department, is to report directly to the Deputy Secretary.

However, the policies of the remaining 10 agencies—Agriculture, HHS, the Departments of Homeland Security (DHS), Housing and Urban Development (HUD), Justice, Labor (Labor), State (State), Treasury; as well as NRC, and the U.S. Agency for International Development (USAID)—did not call for their CIOs to directly report to the heads of their agencies or their deputies. Instead, these agencies directed their CIOs to report to officials that are subordinate to the heads of the agencies and their deputies. For example, the DHS CIO is to report to the Undersecretary for Management.

- **Provide input into bureau CIO ratings.** The policies of slightly more than half of agencies with bureau CIOs (9 out of 14 agencies[43]) addressed CIOs' responsibilities for providing input into the performance ratings of bureau CIOs. For example, according to a Justice order on IT management, the CIO is to engage in the evaluation of bureau CIO performance. However, 5 agencies—the Department of Housing and Urban Development (HUD), Agriculture, Defense, DHS, and Treasury—did not have policies that addressed this responsibility.

Conversely, the remaining 17 responsibilities were fully addressed in the policies of less than half of the applicable agencies. For example:

- **Evaluate IT investments according to risk (IT Dashboard CIO ratings).** Twelve agencies' policies fully addressed the role of their CIOs in evaluating IT investments according to risk. For

[42] The law requires the CIO to report directly to the agency head and OMB's implementing guidance defines the agency head as the overall leader of the agency (e.g., secretary) or that leader's deputy (e.g., deputy secretary) who acts on behalf of the agency's overall leader. OMB, *Management and Oversight of Federal Information Technology, Memorandum* M-15-14 (Washington, D.C.: June 10, 2015).

[43] As previously mentioned, this responsibility does not apply to the 10 agencies that do not have bureau CIOs: the Departments of State and Veterans Affairs, as well as the Environmental Protection Agency, General Services Administration, Office of Personnel Management, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

example, according to the Social Security Administration's (SSA) Capital Planning and Investment Control policy, the CIO is responsible for providing an overall rating for all major IT investments[44] based on the CIO's assessment of the risk and the investment's ability to accomplish its goals. However, the policy of one agency—DHS—partially addressed this responsibility. Specifically, although DHS has established a process for assessing risks of major IT investments, the CIO is no longer primarily responsible for the evaluations or associated risk ratings that are publicly reported for certain major IT investments. Eleven other agencies—the Department of Commerce (Commerce), HHS, HUD, State, VA, the General Services Administration (GSA), NASA, the National Science Foundation (NSF), the Office of Personnel Management (OPM), the Small Business Administration (SBA), and USAID—did not address this responsibility.

- **Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities.** The policies of 6 agencies fully addressed the responsibility of their CIOs to ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities. For example, according to Justice's cybersecurity policy, the CIO is responsible for ensuring that senior agency officials provide cybersecurity protections across agency-wide systems. However, the policies of the remaining 18 agencies—the Departments of Education (Education) and Transportation (Transportation); as well as Agriculture, Commerce, Energy, HHS, DHS, HUD, Labor, State, Treasury, GSA, NASA, NSF, NRC, OPM, SBA, and USAID—did not address this responsibility in their policies.
- **Maintain an inventory of data centers**. Three agencies had policies that fully addressed the responsibility of their CIOs to maintain an inventory of data centers. For example, NRC's data center consolidation guidance calls for the CIO to develop a comprehensive inventory of the data centers owned, operated, or maintained by or on behalf of the agency. However, the policies of

[44] According to OMB, a major IT investment is a system or an acquisition requiring special management attention because of its importance to the mission or function of the government; significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; unusual funding mechanism; or is defined as major by the agency's capital planning and investment control process.

the remaining 19 agencies—[45] the Department of the Interior (Interior); as well as Agriculture, Commerce, Energy, HHS, DHS, Justice, Labor, Transportation, Treasury, VA, the Environmental Protection Agency (EPA), GSA, NASA, NSF, OPM, SBA, SSA, and USAID—did not address this responsibility.

- **Benchmark agency processes against private and public sector performance.** One agency—Justice—had policies that partially addressed the responsibility of the CIO to benchmark agency performance processes against private and public sector performance. Specifically, although Justice established policies that call for the CIO to benchmark against public sector performance, the policies did not describe the CIO's role for benchmarking against private sector performance. The policies of the remaining 23 agencies—Agriculture, Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID—did not address this responsibility.

Officials from 11 of the selected agencies acknowledged that their policies did not fully address all of the key CIO responsibilities and officials from 12 of the agencies indicated that they are working to update aspects of their policies to better address the roles of their CIOs. For example, in July 2017, NASA stated that it was working to update its procedural requirements on IT management to address the role of the CIO with regard to IT workforce responsibilities.

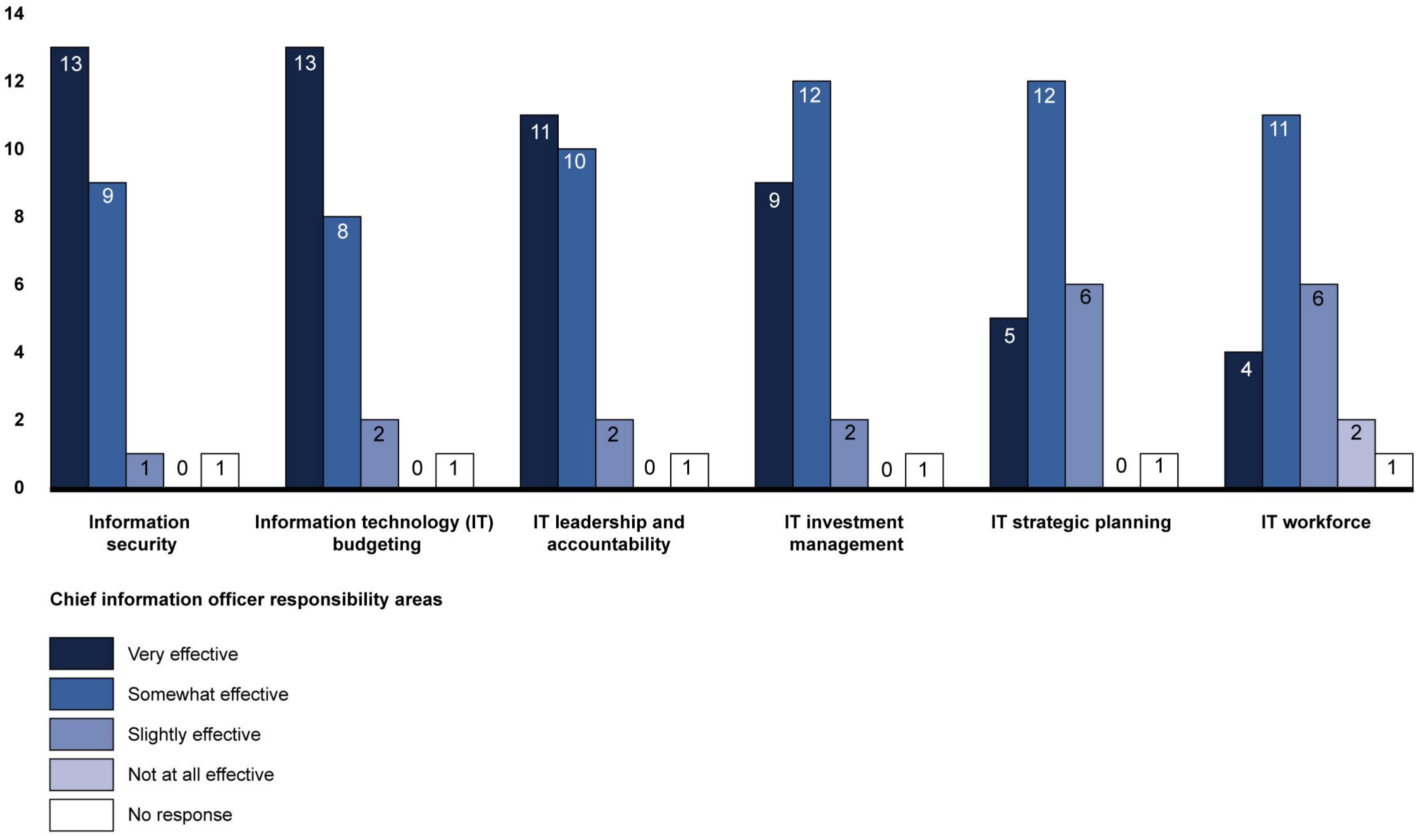
In addition, officials from most agencies stated that their CIOs are implementing the responsibilities even when not required in their agencies' policies. For example, 5 agencies provided their data center optimization strategic plans as evidence that their CIOs are maintaining strategies to consolidate and optimize their data centers.

However, according to their responses, the 24 CIOs that we surveyed noted that they were not always very effective in implementing the six IT management areas. Specifically, at least 10 CIOs indicated that they were less than very effective for each of the six areas of responsibility. For example, although 13 CIOs indicated that they were very effective in carrying out their information security and IT budgeting responsibilities, 10 CIOs noted that they were less than very effective at implementing these

[45] This responsibility does not apply to Education and HUD because these agencies do not have any agency-owned data centers.

two areas of responsibility. In addition, 18 CIOs reported that they were less than very effective at implementing IT strategic planning and 19 CIOs indicated that they were less than very effective at implementing IT workforce responsibilities. Figure 3 depicts the extent to which CIOs reported their effectiveness in implementing the six areas of responsibility and appendix V contains the CIOs' responses to our survey.

**Figure 3: Extent to Which Agency Chief Information Officers (CIO) Reported Effective Implementation of Six Responsibility Areas, Presented from Most Effective to Least Effective Area**



Source: Chief information officer responses to GAO survey. | GAO-18-93

Until agencies fully address the role of CIOs in their policies, agencies will be limited in addressing long-standing IT management challenges.

Beyond the actions of the agencies, however, shortcomings in agency policies also are partially attributable to two weaknesses in OMB's guidance. Specifically, OMB's guidance (1) does not comprehensively address all CIO responsibilities and (2) does not ensure that CIOs have a significant role in decision making and oversight.

- **OMB's guidance does not comprehensively address all CIO responsibilities.** Of the 35 responsibilities in our evaluation framework, OMB's guidance does not address 12 of them.[46] Correspondingly, the majority of the agencies' policies did not fully address 10 of these 12 responsibilities.[47]

Of particular concern is the IT workforce area, wherein OMB's guidance does not address three of the four related responsibilities. The corresponding policies at 18 agencies either minimally addressed or did not address the role of the CIO for this area. For example, 19 agencies' policies had not addressed their CIOs' role in annual assessments of IT management and skill requirements and the remaining 5 agencies had only partially addressed this responsibility.

- **OMB's guidance does not ensure that CIOs have a significant role in decision making and oversight.** OMB's guidance does not fully explain how agencies are to address two of the key CIO responsibilities in FITARA: ensuring CIOs are to have a significant role in (1) IT planning, programming, and budgeting decisions and (2) execution decisions and the management, governance, and oversight processes related to IT. In particular, OMB's guidance calls for CIOs to, among other things, "approve the IT components of any plans through a process balancing IT investments with other uses of agency funding." However, this guidance does not identify what types of plans are to be approved or how implementation will ensure that CIOs have a significant role in IT planning, programming, and budgeting decisions.

[46] The 12 responsibilities not addressed by OMB's guidance are: (1) assume responsibility and accountability for IT investments; (2) establish goals for improving agency operations through IT; (3) measure performance of how well IT supports agency programs; (4) prepare an annual report on the progress in achieving the goals; (5) benchmark agency processes against private and public sector performance; (6) ensure that agency processes are analyzed and revised as appropriate before making significant IT investments; (7) assess annually the extent to which agency personnel meet IT management knowledge and skill requirements; (8) annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies; (9) report annually to the head of the agency on progress made in improving IT personnel capabilities; (10) coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented; (11) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out their information security responsibilities; and (12) ensure that all personnel are held accountable for complying with the agency-wide information security program.

[47] The policies for 15 agencies fully addressed the role of their CIOs for establishing goals for improving agency operations through IT. In addition, the policies for 22 agencies fully addressed the role of their CIOs for assuming the responsibility for IT investments.

> Similarly, OMB's guidance calls for CIOs to participate on governance boards that review IT resources, including bureau investment review boards. However, the guidance does not describe the authority that CIOs are to have on the governance boards and, thus, is unclear as to whether this participation would provide a significant role for CIOs. For example, Agriculture's CIO (or that official's designee) is a non-voting member on 19 of the department's 23 governance boards that review IT resources. However, it is unclear whether non-voting membership on a board constitutes participation under OMB's guidance and whether non-voting membership would provide a significant role for the CIO in IT governance and oversight processes.
>
> Conversely, Transportation's CIO (or that official's designee) is the chair or voting member of 12 of the department's 14 IT governance boards. This example suggests that the Transportation CIO likely has adequate authority on the IT governance boards where that official is the chair or a voting member and that this authority is consistent with OMB's guidance.

In a written response regarding our preliminary findings, OMB stated that the agency CIO is ultimately responsible and accountable for all IT across the agency and, as such, it is important that the CIO's role in governance adequately addresses this expectation. OMB added that, in the specific case where an agency CIO does not have a role that enables that official to make decisions, accept and manage risks, and ensure adequate resource allocation, the CIO's governance role is not adequate. In addition, OMB stated that federal law and OMB recognize that agencies have different operating structures and that a one-size-fits-all approach is not realistic and would not be applicable or effective. OMB added that it has provided agencies the opportunity to determine what is appropriate for each of their respective agencies.

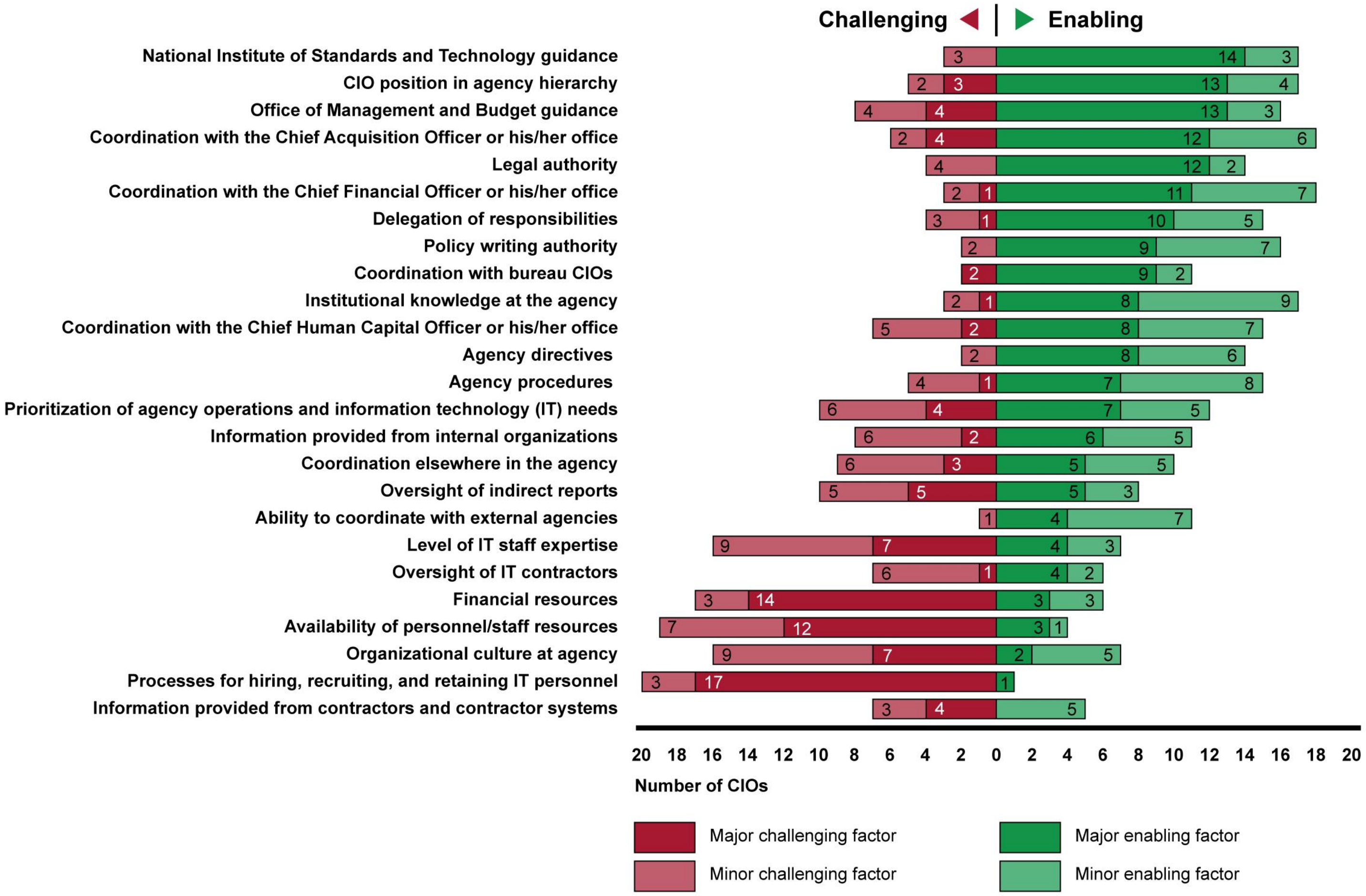
We agree that the agency CIO's role in IT governance should ensure that the CIO is responsible and accountable for all IT across their agencies. However, OMB's guidance has not comprehensively and clearly addressed how agencies are to meet this expectation. In the absence of comprehensive and clear guidance from OMB for all responsibilities, CIOs will not be positioned to effectively acquire, operate, maintain, and secure their IT systems.

## Federal Agency CIOs Identified a Number of Factors That Enabled and Challenged Their Ability to Effectively Manage IT

Of 25 potential factors presented in our survey that could be associated with IT management, agency CIOs identified a number of them as being major enablers of their ability to effectively manage IT. For example, 5 factors were cited by at least half of the 24 CIOs as major enablers. The CIOs also identified several of the factors as being major challenges to effectively implementing their responsibilities. For instance, 3 factors were identified by at least half of the CIOs as major challenges.

Figure 4 shows the extent to which the 24 CIOs reported the 25 factors as enabling and challenging their ability to effectively manage IT. (These factors are also presented in appendix V, which contains the detailed results of our survey.)

Figure 4: Extent to Which 24 Chief Information Officers (CIO) Reported Factors as Enabling and Challenging, Presented from Most Enabling to Least Enabling Factor



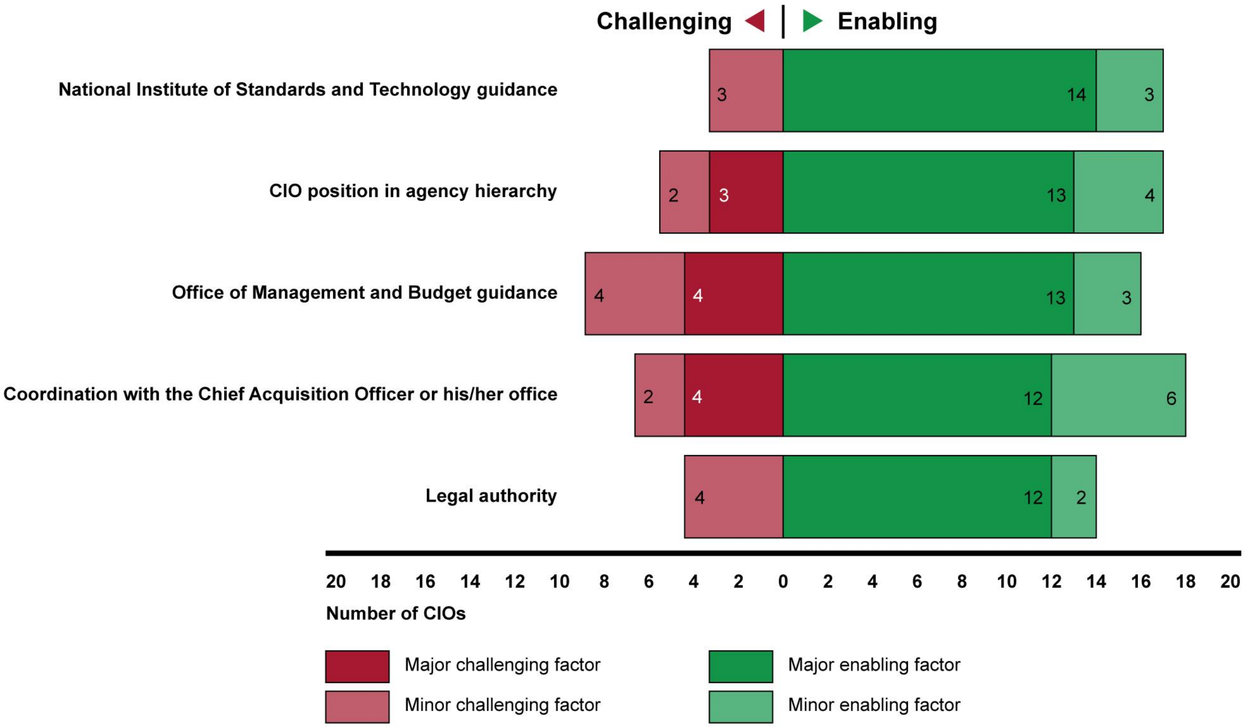
Source: Chief information officer responses to GAO survey. | GAO-18-93

Note: This figure does not depict the number of non-responses for each factor, responses where CIOs identified factors as neither enabling nor challenging, and responses where CIOs identified factors as not applicable.

## Five Factors Were Commonly Identified by CIOs as Enabling Effective IT Management

Of the 25 potential factors, 5 were cited by at least half of the 24 CIOs as major factors that have enabled their ability to effectively carry out their key IT management responsibilities: (1) National Institute of Standards and Technology (NIST) guidance, (2) the CIO's position in the agency hierarchy, (3) OMB guidance, (4) coordination with the Chief Acquisition Officer (CAO), and (5) legal authority. Figure 5 depicts the degree to which the CIOs found these 5 factors to be enabling (along with the extent to which these same factors were viewed as challenging by other CIOs).

**Figure 5: Factors Commonly Identified by at Least Half of the Selected Chief Information Officers (CIO) as Enabling Their Effective Management of Information Technology (IT), Presented from Most Enabling to Least Enabling Factor**



Source: Chief information officer responses to GAO survey. | GAO-18-93

Note: This figure does not depict the number of non-responses for each factor, responses where CIOs identified factors as neither enabling nor challenging, and responses where CIOs identified factors as not applicable.

Half or more of the CIOs commonly identified important benefits associated with the five major enabling factors:

- **NIST guidance.** According to 14 CIOs that responded to our survey, NIST guidance was a major factor that enabled them to effectively carry out their IT management responsibilities—especially the management of information security. One CIO stated that NIST guidance is clear, explains why security activities are necessary and important, and helps facilitate conversations with business and system owners about security. Another CIO stated that NIST guidance provides a common baseline for security and privacy controls. An additional CIO reported that the guidance has helped the agency to improve its information security program by describing how to implement controls for securing information systems and the process for granting authority to operate.

- **CIO position in agency hierarchy.** Thirteen CIOs reported that the CIO's position in the agency hierarchy was a major factor that enabled them to effectively carry out their responsibilities.[48] Five respondents identified several specific benefits related to this factor and highlighted the importance of reporting to the head of the agency or that leader's deputy. For example, one CIO attributed much of the agency's success in managing IT to good relationships that the CIO had with the agency head and that official's deputy. The CIO also noted that being a part of the Secretary's senior leadership team had allowed for a better understanding of the priorities of the agency's political appointees. Another CIO noted the importance of having the agency head support the CIO's decisions to other senior staff. Yet another CIO indicated that support from the head of the agency had enabled that official to cancel a troubled project and reallocate that funding to critical information security improvements on another effort.

In addition, one CIO highlighted the importance of having all chief "X" officers (CXO)[49] report to the same official. In particular, this CIO stated that having all CXOs report to its agency's Under Secretary for Management has been very beneficial because it encourages these officials to develop integrated priorities and work together to achieve them.

[48] Although 13 CIOs reported this factor as a major enabler, 3 CIOs responded that the CIO position in the agency hierarchy was a major challenge. One CIO explained that there are multiple layers of management between the CIO and the agency head, and that it can be challenging to communicate IT issues to this official. To request a meeting, the CIO must first develop a briefing paper that explains the purpose of the meeting. This paper is then reviewed by multiple individuals in the bureau and the office of the agency head before the meeting can be approved.

[49] CXO, or chief "X" officer, is a generic term for job titles where "X" represents a specific, specialized position that serves the entire organization, such as the chief information officer, chief financial officer, chief human capital officer, chief procurement officer, chief performance officer, chief technology officer, chief information security officer, or chief management officer.

- **OMB guidance.** Thirteen CIOs responded that OMB guidance was a major enabler to effectively carrying out their responsibilities.[50] One CIO highlighted OMB's FITARA guidance, noting that it has helped to provide the CIO a significant role in IT budgeting decisions. Another CIO indicated that OMB guidance ensures the agency is aligned with the administration's priorities and perspective. One other CIO stated that the guidance is helpful because it provides a framework for effectively managing IT and cybersecurity, as well as for purchasing commodity IT in bulk.[51]
- **Coordination with the CAO.** For 12 CIOs, coordination with the agency's CAO was a major enabler to carrying out their responsibilities.[52] Two of these respondents stated that the CAO is a critical partner that provides the CIO with greatly increased visibility. One respondent further noted that the CAO provides the CIO with insight into IT acquisitions and spending that are typically not highlighted as part of agency IT review processes.[53] Another CIO noted that a great relationship with the CAO allowed the CIO to quickly identify and resolve acquisition problems.
- **Legal authority.** Twelve CIOs highlighted legal authority as a major enabler to carrying out their responsibilities. In this regard, one CIO stated that FITARA is the cornerstone of agency policies,

[50] Although 13 CIOs reported this factor as a major enabler, 4 CIOs responded that OMB guidance was a major challenge to carrying out their responsibilities. One CIO stated that OMB's IT budget guidance is typically released too late in the budget cycle. That CIO also noted that OMB's guidance is not always clear and is not tailored to the significant differences between larger, more federated agencies and smaller, non-federated agencies. Another CIO stated that OMB guidance often provides new direction to agencies without consideration of needed resources or funding.

[51] According to OMB, commodity IT includes services such as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (email, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions).

[52] Conversely, four CIOs responded that coordination with the CAO was a major challenge to carrying out their responsibilities. One CIO stated that the CAO office is understaffed with high attrition and contracting officers give inconsistent responses. Another CIO indicated that the CAO office does not have the skills and resources needed to effectively acquire Agile software development services.

[53] By contrast, in our January 2018 report on agencies' efforts to appropriately involve CIOs in reviewing IT acquisitions, we reported that the majority of the selected 22 agencies that did not identify the $4.5 billion in IT obligations also did not follow OMB's guidance to have the CAO identify all IT acquisitions for CIO review and approval. GAO, *Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions*, GAO-18-42 (Washington, D.C.: Jan. 10, 2018).

provides decision-making authority, and increases budget visibility. Another stated that the CIO's legal authority under FITARA has eliminated pushback from other organizations and given the CIO the ability to access key program information.

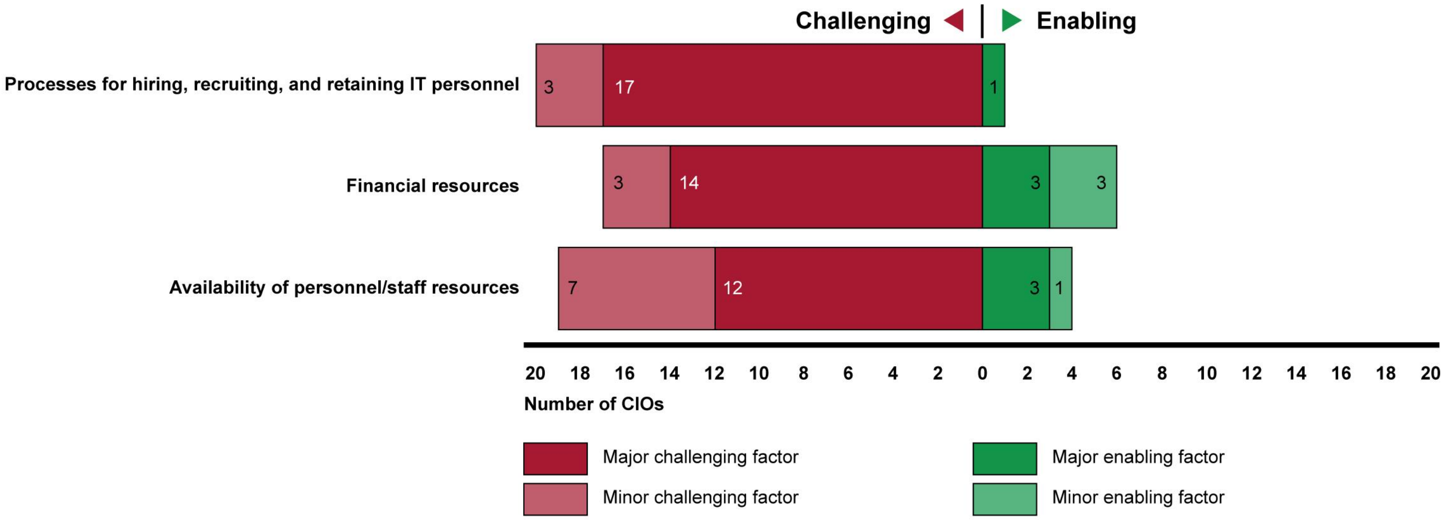
Many of these factors that were cited by 12 or more of the CIOs that we surveyed also were highlighted during our 2016 forum that explored the improvements needed for IT acquisitions and operations.[54] In particular, forum participants discussed the importance of CIOs obtaining support from agency leadership and OMB to help ensure effective IT governance. Among other things, they noted that agencies could benefit from support from the agency heads to ensure that CIOs have adequate authority to effectively govern IT investments.

## Three Factors Were Commonly Identified by CIOs as Challenging IT Management

Of the 25 factors, 3 were cited by at least half of the 24 CIOs as major factors that have challenged their ability to effectively carry out their key IT management responsibilities: (1) processes for hiring, recruiting, and retaining IT personnel; (2) financial resources; and (3) the availability of personnel/staff resources. Figure 6 depicts the factors and shows how many CIOs cited them as challenging (as well as how many CIOs cited them as enabling).

[54] GAO-17-251SP.

**Figure 6: Factors Commonly Identified by at Least Half of the Selected Chief Information Officers (CIO) as Challenges to Their Effective Management of Information Technology (IT), Presented from Most Challenging to Least Challenging Factor**



Source: Chief information officer responses to GAO survey. | GAO-18-93

Note: This figure does not depict the number of non-responses for each factor, responses where CIOs identified factors as neither enabling nor challenging, and responses where CIOs identified factors as not applicable.

Among half or more of the CIOs, the three factors were commonly identified as major challenges in the following ways:

- **Processes for hiring, recruiting, and retaining IT personnel.** Seventeen CIOs reported that the processes for hiring, recruiting, and retaining IT personnel were a major challenging factor.[55] Nine CIOs explained that their agencies' hiring processes are slow and inefficient, which makes it difficult for the CIOs to hire the staff with needed skills and experience. For example, one CIO stated that many strong candidates have dropped out of the agency's hiring process due to its unreasonable length.

Separately, five CIOs indicated that they could not offer salaries for candidates with high-demand technical skills that are competitive with

[55] Although a majority of CIOs reported this factor as a major challenge, one CIO stated that the processes for hiring, recruiting, and retaining IT personnel were a major enabling factor. The CIO stated that the agency used direct hire authority to employ many staff after it held a technology event. In addition, the CIO explained that the agency quickly retained a number of experts for its digital service team using Schedule A excepted service hiring authority.

the private sector and several federal agencies with authority to pay higher salaries. For example, one CIO stated that the agency has difficulty competing with the private sector for IT talent because the private sector salaries are typically higher than what the agency can offer. Another CIO stated that a key employee left the agency to work for an agency with authority to pay higher salaries. Lastly, one CIO noted that the CIO does not have a role in the hiring of IT personnel.

Further compounding this issue is the lack of consistent leadership in the CIO position. We noted previously that CIOs and former agency IT executives believed it was necessary for a CIO to stay in office for 3 to 5 years to be effective and 5 to 7 years to fully implement major change initiatives in large public sector organizations.[56] However, the median tenure for permanent and acting agency CIOs who had completed their time in office was about 20 months between 2012 and 2017.[57] In addition, the median tenure for permanent agency CIOs who had completed their time in office was about 32 months between 2012 and 2017. (See appendix II for further information on the tenure of CIOs.)

Challenges in attracting and retaining qualified CIOs were highlighted during our 2016 forum that explored the improvements needed for IT acquisitions and operations.[58] For example, a participant suggested that 5-year term appointments for CIO positions would allow for more time to influence change within agencies.

- **Financial resources.** Fourteen CIOs cited financial resources as a major challenge to effectively implementing their IT management responsibilities.[59] Six CIOs indicated that they did not have sufficient budgets to fully staff their offices, which impeded their ability to oversee IT investments and security

[56] GAO-04-823.

[57] This reflects the tenure of CIOs who had completed their time in office between January 1, 2012, and November 30, 2017.

[58] GAO-17-251SP.

[59] Although a majority of CIOs reported this factor as a major challenge, three CIOs cited financial resources as a major enabler. For example, one CIO told us that the agency receives a single appropriation for all agency IT spending, which reduces the amount of time needed for the CIO to review and approve the IT budget and allows the CIO to spend time on other important areas, such as modernizing legacy systems.

activities of bureau organizations.[60] For example, one CIO noted that the agency's overall IT spending had increased by more than 40 percent over the past 5 years, but the budget for operating the Office of the CIO had remained the same. That official felt that the financial resources for the Office of the CIO were not sufficient to effectively oversee and support the agency's IT investments and information systems. Three other CIOs stated that their agencies have not been provided any additional funding to implement recent IT management legislation and OMB guidance.

In addition, seven CIOs indicated that inadequate agency IT budgets had impeded their ability to modernize legacy IT systems, consolidate data centers, implement cloud computing solutions,[61] and improve their cybersecurity postures. For example, one CIO stated that about 90 percent of the agency's budget is spent on operating and maintaining IT, leaving only 10 percent of the budget for new development, modernization, and enhancements. This official explained that having a relatively small budget for new development makes it difficult to effectively modernize legacy systems and improve the agency's cybersecurity posture.

Further, two CIOs noted that they did not have adequate visibility and control over their agencies' IT spending. One CIO reported having control over about 5 percent of the agency's IT spending. Another CIO stated that there was a lack of complete insight into IT spending at bureaus, especially for spending outside the control of bureau CIOs.

- **Availability of personnel/staff resources.** Twelve CIOs cited the availability of personnel or staff resources as a major challenge.[62]

[60] Federal law emphasizes the importance of agency CIOs having responsibility and accountability for all IT across their agencies. However, as previously noted, agencies did not fully address in agency policies the role of their CIOs consistent with federal law. Fully addressing the role of agency CIOs consistent with federal law could better position them to effectively prioritize IT spending across their agencies. In addition, Congress took legislative action by way of the MGT Act to authorize the availability of funding to help further agencies' efforts to modernize IT. Specifically, the law authorizes agencies to establish working capital funds for use in transitioning from legacy IT systems, as well as for addressing evolving threats to information security.

[61] According to NIST, cloud computing is a means "for enabling on-demand access to shared and scalable pools of computing resources with the goal of minimizing management effort or service provider interaction."

[62] Although 12 CIOs reported this factor was a major challenge, 3 CIOs cited availability of personnel as a major enabling factor. For example, one CIO stated that the agency was able to effectively hire IT personnel because the CIO hired and embedded personnel within the agency's human resources office who were dedicated to managing IT workforce issues.

For example, similar to the financial resources challenge, three CIOs stated that they did not have sufficient budgets for Office of the CIO staffing. As such, these officials said they lacked staff to oversee IT investments and security activities of bureau organizations.

All three major challenging factors are consistent with our 2016 forum regarding improvements needed for IT acquisitions and operations, as well as our 2004 and 2011 reports on CIOs.[63] In particular, the forum participants suggested giving CIOs more flexibilities in order to better hire, recruit, and retain IT personnel. In addition, our 2004 and 2011 reports on CIOs' roles and responsibilities described similar challenges, including limitations in financial resources and processes for hiring, recruiting, and retaining IT personnel.

## OMB's Guidance Does Not Fully Address Challenges Commonly Identified by CIOs

In accordance with its responsibility to provide centralized management guidance and oversight for all executive branch agencies, OMB, in coordination with other agencies, has issued guidance aimed at addressing the three commonly identified CIO challenges. For example, with regard to the two challenges related to IT personnel—processes for hiring, recruiting, and retaining IT personnel; and the availability of personnel and staff resources—OMB issued its 25-point plan for IT reform in 2010 and outlined several action plans to build workforce capabilities, including acquisition and program management.[64] In addition, in October 2015, OMB issued its Cybersecurity Strategy and Implementation Plan, which, among other things, tasked OPM to provide agencies with information regarding hiring, pay, and leave flexibilities to help recruit and retain individuals in cybersecurity positions.[65] Further, OMB and OPM issued the Federal Cybersecurity Workforce Strategy in July 2016, detailing government-wide actions to recruit, develop, and

[63] GAO-17-251SP, GAO-11-634, and GAO-04-823.

[64] OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

[65] OMB, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, M-16-04 (Washington, D.C.: Oct. 30, 2015).

retain a workforce in key functional areas to address complex and ever-evolving cyber threats.[66]

With regard to the third challenge on financial resources, staff in OMB's Office of E-Government and Information Technology stated that OMB has reformed IT investment management processes. For example, OMB's fiscal year 2019 IT budget guidance[67] calls for agencies to begin reporting budget and spending information using standard categories of IT costs (e.g., labor, hardware, and software) and resources (e.g., data center, storage, and network).[68] OMB's guidance calls for agencies to increase reporting on new IT cost categories incrementally over the next several years, with reporting on all cost categories scheduled for fiscal year 2021. In addition, in February 2018, OMB issued guidance for agencies to implement the MGT Act.[69] The guidance was intended to provide agencies additional information regarding the Technology Management Fund, and the administration and funding of the related IT Working Capital Funds.

Further, in its fiscal year 2018 IT budget guidance to agencies, OMB called for agencies to report to OMB the dollar amounts for each IT investment over which their CIOs have authority.[70] Of the 23 agencies that reported such data for fiscal year 2018,[71] 8 reported that their CIOs had authority over all of the agencies' IT spending, 5 reported that CIOs had authority for between 50 and 100 percent of the IT spending, and 10 agencies reported that CIOs had authority for less than 50 percent of the IT spending. By collecting this information, OMB stated that it hopes to

[66] OMB and OPM, *Federal Cybersecurity Workforce Strategy*, M-16-15 (Washington, D.C.: July 12, 2016).

[67] OMB, *FY2019 IT Budget – Capital Planning Guidance*.

[68] These standard categories are part of Technology Business Management, a framework developed and managed by the Technology Business Management Council.

[69] OMB, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

[70] OMB, *FY2018 IT Budget – Capital Planning Guidance*. OMB's latest guidance includes this same request for agency information on CIO authority. OMB, *FY2019 IT Budget – Capital Planning Guidance*.

[71] In an August 2016 letter to OMB, Defense stated that it would not submit this information to OMB because it had more complex IT management than a typical civilian agency, the information would be burdensome to collect, and the information would not result in an accurate representation of the department's governance system or the CIO's impact.

measure CIO authority over IT spending and help agencies to improve that authority.

Nevertheless, OMB's guidance does not fully address the three commonly identified CIO challenges in our survey. With respect to the two challenges related to IT personnel, as previously mentioned, OMB's guidance does not address all CIO responsibilities. Specifically, OMB's guidance does not address the responsibilities to annually (1) assess the extent to which agency personnel meet IT management knowledge and skill requirements, (2) develop strategies for hiring and training to rectify any knowledge and skill deficiencies, and (3) report to the agency head on progress made in improving these responsibilities. As we stressed, until OMB updates its guidance to address these responsibilities, CIOs may not have the personnel needed to effectively acquire, maintain, and secure their IT systems.

Further, regarding the financial resources challenge, as previously mentioned, OMB recently required agencies to provide data on CIO authority over IT spending. For example, of the 8 agencies that reported that their CIOs had 100 percent authority over the agencies' IT spending, 7 agencies defined authority as their CIOs coordinating with bureaus. By contrast, of the 10 agencies that reported CIO authority over less than 50 percent of IT spending, 2 stated that, although their CIO coordinates with bureaus, the CIOs do not have authority over bureau-level IT spending.

These widely varying levels of CIO authority over IT spending are, in part, because OMB's guidance did not completely define the authority CIOs should have over IT spending. In a written response regarding our preliminary findings, OMB stated that the agency CIO is ultimately responsible and accountable for all IT across the agency and, as such, it is important that the CIO's role in governance adequately addresses this expectation. OMB added that, in the specific case where an agency CIO does not have a role that enables that official to make decisions, accept and manage risks, and ensure adequate resource allocation, the CIO's governance role is not adequate. We agree with OMB and believe that including such language in OMB's guidance would help to address the issue of CIOs' authorities.

## Conclusions

Over the past two decades, Congress has assigned critical federal IT responsibilities to CIOs. However, the policies of each of the 24 agencies did not fully address their CIOs' key responsibilities for IT management. Although officials from most agencies stated that their CIOs were implementing the responsibilities even when not addressed in policy, the 24 CIOs acknowledged in our survey that they were not always very effective in implementing all of their responsibilities. Further, the shortcomings in agencies' policies are attributable, at least in part, to incomplete guidance from OMB. Until OMB improves its guidance to clearly address all CIO responsibilities and agencies fully address the role of CIOs in their policies, CIOs will be limited in effectively managing IT and addressing long-standing IT management challenges.

The CIOs we surveyed identified a number of factors that enabled and challenged their ability to effectively manage IT. Most CIOs felt enabled by OMB and NIST guidance, their position in the agency hierarchy, and authority given to them by Congress. This underscores the importance of guidance and building relationships within leadership teams. However, agencies continue to lack consistent leadership in the CIO position. Further, the majority of CIOs continue to report major challenges related to their agencies' IT workforces and financial resources. While OMB has taken steps to address these challenges, further strengthening its efforts to improve CIO authority over IT spending could better position agencies to effectively manage IT.

## Recommendations for Executive Action

We are making a total of 27 recommendations to federal agencies—3 recommendations to OMB and 1 each to the 24 agencies.

We are making the following 3 recommendations to OMB:

- The Director of the Office of Management and Budget should issue guidance that addresses the 12 CIO responsibilities discussed in this report that are not included in existing OMB guidance—in particular those relating to IT workforce matters. (Recommendation 1)
- The Director of the Office of Management and Budget should update existing guidance to clearly explain how agencies are to address the role of CIOs to comply with the statutory requirements for CIOs to have a significant role in (1) budgeting decisions and (2) the management, governance, and oversight processes related to IT. (Recommendation 2)

- The Director of the Office of Management and Budget should define the authority that CIOs are to have when agencies report on CIO authority over IT spending. (Recommendation 3)

We are making a recommendation to each of the 24 departments and agencies in our review. Specifically:

- The Secretary of Agriculture should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 4)
- The Secretary of Commerce should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 5)
- The Secretary of Defense should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 6)
- The Secretary of Education should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 7)
- The Secretary of Energy should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 8)
- The Secretary of Health and Human Services should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 9)
- The Secretary of Homeland Security should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 10)
- The Secretary of Housing and Urban Development should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 11)
- The Secretary of the Interior should ensure that the department's IT management policies address the role of the CIO for key

responsibilities in the five areas we identified. (Recommendation 12)

- The Attorney General should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 13)
- The Secretary of Labor should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 14)
- The Secretary of State should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 15)
- The Secretary of Transportation should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 16)
- The Secretary of the Treasury should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 17)
- The Secretary of Veterans Affairs should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the four areas we identified. (Recommendation 18)
- The Administrator of the Environmental Protection Agency should ensure that the agency’s IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 19)
- The Administrator of the General Services Administration should ensure that the agency’s IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 20)
- The Administrator of the National Aeronautics and Space Administration should ensure that the agency’s IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 21)

- The Director of the National Science Foundation should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 22)
- The Chairman of the Nuclear Regulatory Commission should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 23)
- The Director of the Office of Personnel Management should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 24)
- The Administrator of the Small Business Administration should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 25)
- The Commissioner of the Social Security Administration should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the five areas we identified. (Recommendation 26)
- The Administrator of the U.S. Agency for International Development should ensure that the agency's IT management policies address the role of the CIO for key responsibilities in the six areas we identified. (Recommendation 27)

## Agency Comments and Our Evaluation

We provided a draft of this report to OMB and the 24 agencies included in our review. Fourteen agencies (Agriculture, Commerce, Education, Energy, HHS, DHS, Interior, Justice, State, VA, NASA, NSF, OPM, and SSA) agreed with our recommendations; 5 agencies (Defense, Transportation, GSA, OMB, and SBA) partially agreed with our recommendations; 1 agency (NRC) disagreed with our recommendation; and 5 agencies (HUD, Labor, Treasury, EPA, and USAID) had no comments on the recommendations.

The following 14 agencies agreed with our recommendations:

- Agriculture agreed with our findings and recommendation. The department stated that it has made great strides in the implementation of FITARA and has embraced the responsibilities, authorities, and accountability provided to the CIO as part of FITARA. The department added that it has taken initial steps to address our recommendation by, for example, establishing a team to update Agriculture's FITARA policy to address CIO authorities.

The department also said that it has established and largely implemented its plan for carrying out OMB's guidance for FITARA and related IT management practices. It noted that we had recently identified the department as having effective practices in the areas of the Federal Data Center Consolidation Initiative[72] and Category Management/Software Licensing Management.[73]

In addition, Agriculture stated that, although its CIO does not report directly to the Secretary or Deputy Secretary, the CIO has direct access to these officials for all IT matters and routinely meets with them to keep them apprised of all aspects of IT across the Agriculture portfolio. However, although Agriculture stated that its CIO has direct access to the Secretary or Deputy Secretary, federal law and OMB guidance require the CIO to report directly to these officials. Until Agriculture ensures that its CIO reports to the Secretary or Deputy Secretary, there is increased risk that its CIO will not be positioned to effectively implement key responsibilities. Agriculture's comments are reprinted in appendix VI.

- Commerce agreed with our recommendation and said it will work to develop a plan in a timely manner to ensure that the department's IT management policies clearly and fully address the role of the CIO for the key responsibilities. Commerce's comments are reprinted in appendix VII.
- Education agreed with our findings and recommendation. The department stated that it had developed various delegation and

[72] In May 2018, we reported that Agriculture had closed 19 of the 35 tiered data centers as of August 2017 and planned to close an additional 9 by September 2018. GAO, *Data Center Optimization*, *Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations*, GAO-18-264 (Washington, D.C.: May 23, 2018). In addition, we reported that, of the $8.72 million that Agriculture had planned to save through the Data Center Optimization Initiation for fiscal years 2016 and 2017, Agriculture achieved $5.71 million in savings.

[73] In May 2014, we made six recommendations to Agriculture to improve its policies and practices for managing software licenses. GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide*, GAO-14-413 (Washington, D.C.: May 22, 2014). As of May 2018, Agriculture has implemented 5 of our recommendations.

policy documents that were intended to empower the CIO to execute all tasks, as described by federal law and OMB guidance. The department added that its CIO is currently performing most of the responsibilities identified in our review, but said Education recognizes that the responsibilities were not explicitly documented in its policies. The department stated that it plans to update its policies to reflect the specific responsibilities that we identified as not addressed.

If Education follows through on its plans to address the role of the CIO across the six areas of CIO responsibility, its CIO should be better positioned to effectively implement key CIO responsibilities. Education's comments are reprinted in appendix VIII.

- Energy concurred with our recommendation to the department. Energy explained that it is working diligently to implement the responsibilities of the CIO, as required by law. The department added that it intends to ensure that its IT management documents and/or policies address the role of the CIO for the five areas that we identified as not addressed. Energy further stated that it expects to complete this documentation process by May 1, 2019.

If Energy follows through on its plans to address the role of the CIO for responsibilities across all of the areas we identified, its CIO should be better positioned to effectively implement key responsibilities. Energy's comments are reprinted in appendix IX.

- HHS concurred with our recommendation and stated that it has made significant progress in ensuring that its CIO's authorities are consistent with FITARA. The department added that it has taken a number of actions to address our findings for the 15 responsibilities we identified as not addressed.

Some of the actions that HHS noted appear to describe the department's efforts to carry out the responsibilities, and do not describe efforts to develop policies that address the CIO's role with regard to the six CIO responsibility areas. It is important that HHS ensures that it develops policies for all key CIO responsibilities in order to position the CIO to address longstanding IT management challenges. HHS's comments are reprinted in appendix X.

- DHS concurred with our recommendation and stated that it is pleased to note our recognition of the policies it created to ensure the role of the CIO is consistent with federal laws and guidance. In addition, the department stated that, subsequent to receiving our draft report for comment, it had updated and revised the delegation of authority from the Under Secretary for Management to the CIO, explicitly authorizing the CIO to exercise the full range of authorities enumerated in FITARA and other statutes. Further, the department stated that it updated directive 142-02, *Information Technology Integration and Management*, to clearly address the CIO responsibilities not fully addressed previously.

We have not yet had the opportunity to examine the updated delegation of authority and directive to determine whether they fully address the role of the CIO for the responsibilities we assessed as having not been addressed. If these policies fully address the role of the agency's CIO, that official should be better positioned to effectively carry out key IT management responsibilities. DHS's comments are reprinted in appendix XI. The department also provided technical comments, which we have incorporated in the report, as appropriate.

- Interior concurred with our recommendation and stated that it believes the department has sufficiently addressed the role of its CIO. Interior added that it will perform a policy analysis review to verify that the CIO authorities are appropriately implemented in accordance with statute and will take corrective actions, as necessary.

If Interior follows through on its plans to address the role of the CIO for responsibilities across all of the areas we identified, its CIO should be better positioned to effectively implement all key responsibilities. Interior's comments are reprinted in appendix XII.

- In comments provided via email on May 8, 2018, a Justice program analyst in the Internal Revenue and Evaluation Office of the Justice Management Division stated that the department concurred with our recommendation.
- VA concurred with our recommendation and stated that, although the CIO is currently implementing most of the responsibilities identified in the draft report, VA acknowledges that many of these responsibilities are not explicitly formalized by departmental policy. VA committed to ensuring that the department's IT management policies will fully address all key IT management responsibilities of federal CIOs. VA's comments are reprinted in appendix XIII.
- State concurred with our recommendation and said the department is committed to its ongoing policy realignment effort to comply with IT management policies that address the role and responsibilities of the CIO. State's comments are reprinted in appendix XIV.

- NASA concurred with our recommendation and stated that the agency is currently updating its policies to address the responsibilities identified in our report. NASA added that it expects to complete these updates by January 18, 2019.

If NASA effectively updates its policies to address the role of the CIO across all areas of responsibility, then its CIO should be better positioned to effectively address longstanding IT management challenges. NASA's comments are reprinted in appendix XV.

- NSF concurred with our recommendation and said it will ensure that the agency's IT management policies address the role of the CIO for the key responsibilities in the five areas we identified. NSF also described additional documentation that it provided as evidence that it has addressed the role of the CIO, such as a process for reviewing and approving reprogramming requests, as well as the agency's updated information security handbook.

Some of the documents NSF provided do not appear to be agency policies, such as the agency's data center consolidation inventory and strategic plan. It is important that NSF ensures that it develops policies for all key CIO responsibilities in order to position the CIO to effectively carry out those responsibilities. NSF's comments are reprinted in appendix XVI. The agency also provided technical comments, which we have incorporated in the report, as appropriate.

- OPM concurred with our recommendation and stated that, it will review and update, as appropriate, the agency's IT management policies to address the role of the CIO for the key responsibilities identified in our report. OPM's comments are reprinted in appendix XVII.
- SSA agreed with our recommendation and stated it continues to make progress in integrating its CIO into managing the areas of IT strategic planning, workforce, budgeting, and investment management. In addition, the agency acknowledged our findings and said it has initiated a timeline to obtain full compliance in all areas identified by our report.

SSA further explained that, as it continues to integrate the CIO into its management practices, the agency is developing a formal policy that addresses the CIO's responsibilities in the areas for which the role of the CIO were not fully addressed. The agency stated that, in March 2018, it completed the first iteration of its new CIO policy, which addressed many of the responsibilities. SSA added that it expects to complete a second iteration of the policy by September 30, 2018, which will fully address all areas of key CIO responsibilities.[74]

If SSA follows through on its plans to address the role of the CIO for responsibilities across all areas, its CIO should be better positioned to effectively implement key responsibilities. SSA's comments are reprinted in appendix XVIII.

In addition, the following five agencies partially agreed with our recommendations:

- Defense agreed with our recommendation related to IT leadership and accountability, partially agreed with our recommendation related to IT strategic planning, partially agreed with our recommendation related to IT workforce, did not agree with our recommendation related to IT investment management, and partially agreed with our recommendation related to information security. Specifically:
  - *Leadership and accountability*. Defense agreed with our recommendation that the department's CIO provide input into bureau CIOs'[75] performance evaluations. According to the department, legislative relief would be required to allow the Defense CIO to approve the selection of CIOs in the three military departments; however, the department said it is in the process of drafting a policy requiring the designation of bureau CIOs to be vetted with the Defense CIO. The department added that this policy would also allow the Defense CIO to provide input into the performance of the bureau CIOs.

    If Defense follows through on its plans to address the role of the department's CIO in providing input on the performance of bureau CIOs, then its CIO should be better positioned to effectively oversee and manage the IT activities of the department's bureaus.
  - *IT strategic planning*. Defense partially agreed with our recommendation related to two responsibilities in the area of IT strategic planning—(1) prepare an annual report on progress in achieving the goals and (2) benchmark agency processes against private and public sector performance. Regarding the first

[74] Further, SSA stated that it created lower-level CIO responsibility policies for the certification of incremental development and IT acquisition approval and provided links to these documents on its public website. We have not yet reviewed these policies.

[75] Defense refers to bureau CIOs as the CIOs of the military departments, or components.

responsibility, Defense stated that it intends to include metrics related to progress in the next version of the department's IRM strategic plan. With respect to the second responsibility, Defense stated that the IT and business system reform team plans to leverage industry and federal benchmarks when conducting research and analyses.

Nevertheless, while Defense's actions describe the department's efforts to carry out the responsibilities, Defense did not describe efforts to develop policies that address the role of the CIO for the responsibilities. Developing such policies is important to ensuring the CIO is effectively positioned to carry out those responsibilities.

- *IT workforce.* Defense partially agreed with our recommendation related to this area. Specifically, Defense agreed with the annual IT workforce review requirements and noted it will incorporate them into related guidance that it is developing.

  However, Defense partially agreed with our finding relating to the Defense CIO reporting annually to the Secretary of Defense on progress made in improving IT personnel capabilities. In particular, Defense explained that, prior to the elimination of requirements under section 10 U.S.C. § 115b, the Secretary of Defense submitted a Strategic Human Capital Plan—which included an appendix on IT workforce developed by the CIO—to Congress on an annual and then biannual basis. Defense added that, because this statutory requirement has been eliminated, the CIO will identify a replacement process to make the Secretary of Defense aware of IT workforce issues and initiatives.

  If Defense follows through on its plans to address the role of the CIO for IT workforce responsibilities, its CIO should be better positioned to effectively assess agency IT workforce needs and develop strategies for meeting those needs.

- *IT Investment management*. Defense did not agree with our assessment that it did not address the role of the CIO for the responsibility to certify that investments are adequately implementing incremental development consistent with OMB capital planning guidance. According to Defense, its Financial Management Regulations require a statement of compliance from each Defense bureau indicating that the bureau CIO certifies the investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB.

We have not yet determined whether the Financial Management Regulations address this responsibility. If this policy fully addresses the role of the CIO, that official should be better positioned to effectively certify that the agency's IT investments are adequately implementing incremental development.

- *Information security.* Defense partially agreed with our recommendation related to reporting annually to the agency head on the effectiveness of the agency information security program. According to Defense, the CIO provides an assessment of the department's information security program to the Secretary and Deputy Secretary on an annual basis. Defense added that this requirement is documented in *Instruction 8500.01*, *Cybersecurity*. In addition, Defense stated that the CIO provides an updated cybersecurity scorecard to the Deputy Secretary of Defense on a monthly basis.

  While Defense's cybersecurity policy calls for the CIOs to report annually on the effectiveness of the department's information security program, it does not address the responsibility to provide the report to the head of the agency. Developing such a policy is important to ensuring that the agency head is better positioned to receive information on the effectiveness of the agency's information security program.

Defense's comments are reprinted in appendix XIX.

- In comments provided via email on May 7, 2018, Transportation's Director of Audit Relations and Program Improvement stated that the department agreed with many of the responsibilities highlighted in our recommendation. However, that official stated that the department does not agree with our assessments in the areas of IT strategic planning, IT budgeting, and IT investment management.

  - *IT strategic planning*. Transportation explained that it provided us with multiple documents demonstrating how the CIO was historically involved in the IT strategic planning process. Transportation added that it believed that it provided sufficient evidence for us to assess the area as being partially addressed.

    However, Transportation did not provide us with policies that address the role of the CIO for the responsibilities associated with IT strategic planning. Thus, we did not change our assessment for this area.

  - *IT budgeting*. Transportation provided a memorandum on its IT spend plan process, which it believed addresses the responsibilities to (1) have a significant role in IT planning, programming and budgeting decisions; and (2) review and approve the IT budget request.

The spend plan process that Transportation provided calls for the Office of the CIO to approve IT purchases for most bureaus.[76] However, the process does not address the role of the CIO for the previously mentioned two responsibilities. In particular, with respect to the first responsibility to have a significant role in IT planning, programming and budgeting decisions, the spend plan does not address two of the three component elements (define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages; and approve the IT components of any plans through a process balancing IT investments with other uses of agency funding).[77] In addition, the spend plan process does not address the CIO responsibility to review and approve the IT budget request. Thus, we did not change our assessment for this area.

- *IT investment management*. Transportation referred to the previously mentioned memorandum on its IT spend plan process and believed this memorandum addresses the responsibility to have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT. In addition, Transportation provided its data center optimization inventory and strategic plan as evidence that it has addressed the responsibilities of maintaining an inventory of data centers and maintaining a strategy to consolidate and optimize data centers.

  With respect to the first responsibility to have a significant role in IT execution decisions, as previously mentioned, although the spend plan process document calls for the CIO to approve IT spending for most bureaus, it does not address the four

[76] The memo does not require the Office of the CIO to approve Federal Aviation Administration IT purchases. By law, the Administrator of FAA is the final authority for carrying out functions relating to the acquisition and maintenance of property, services, and equipment of the Administration. 49 U.S.C § 106 (f)(2).

[77] Transportation addressed the role of the CIO for the third component element (participate in the planning, programming, and budgeting stages for programs that include IT resources).

component elements of this responsibility.[78] Regarding the latter responsibilities to maintain a data center inventory and strategy, the documents Transportation provided do not call for the CIO to maintain an inventory and strategy for consolidating and optimizing data centers. Developing such a policy is important to ensure that Transportation continues to carry out its responsibilities for consolidating and optimizing data centers. Thus, we did not change our assessments for these responsibilities.

- GSA partially agreed with our findings and noted it recognizes that there are gaps in its formal policy directives and that it has already begun to update and implement policies in order to fully address the role of the CIO consistent with federal law and guidance in the key areas identified in this report.

However, GSA further explained that it respectfully challenges the report's underlying premise that all individual responsibilities must be codified into agency policy in order to assure efficacy of implementation. GSA requested that we consider that its CIO implements the responsibilities and described examples in the areas of IT strategic planning, workforce, budgeting, and investment management. For example, with respect to IT strategic planning, GSA stated that it published and regularly updates both an IT strategic plan and a data center optimization initiative strategic plan in compliance with existing OMB guidance.

Further, GSA disagreed with our finding that its IT security policies did not address the role of the CIO for the responsibility to ensure that all personnel are held accountable for complying with the agency-wide information security program. GSA noted that its policy *CIO 2100.1K, GSA Information Technology (IT) Security Policy,* June 30, 2017, requires all employees and contractors to follow specific processes to ensure the safeguarding of GSA resources, and holds all personnel accountable for following and enforcing the IT security program. GSA added that, because this policy ensures that all personnel are held

[78] As discussed in more detail in appendix IV, the four elements of the responsibility to have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT are as follows (1) establish and maintain a process to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective; (2) define agency-wide policy for the level of detail of planned IT expenditure reporting; (3) define overall policies for capital planning, enterprise architecture, project management, and reporting for IT resources; and (4) participate on governance boards that include IT resources, including bureau investment review boards.

accountable for complying with the agency-wide security program, GSA respectfully requests that this finding be changed to show that the role of the CIO has been fully addressed.

We agree that, with strong and consistent leadership from CIOs, these responsibilities can be carried out effectively, even when not required in their agencies' policies. However, as we and others have previously stated,[79] in the absence of policies, processes are usually ad hoc and chaotic and success in these organizations depends on the competence and heroics of people in the organization. By contrast, organizations with defined policies are more likely to establish and implement effective processes for carrying out responsibilities.

Correspondingly, the two areas in which CIOs stated they were least effective—IT strategic planning and IT workforce—were the same two areas for which the majority of the agencies minimally addressed or did not address the role of their CIOs. Moreover, as noted previously, many agencies have not had consistent leadership in the CIO position. As such, developing policies that address the role of the CIO for key responsibilities would increase the likelihood that these responsibilities are implemented effectively—especially for those agencies lacking consistent CIO leadership. Therefore, we did not change our assessments for these areas.

With respect to the responsibility to ensure that all personnel are held accountable for complying with the agency-wide information security program, GSA's IT Security Policy requires all personnel to follow the agency's IT security policies and states that disciplinary action may be taken where the policies are not followed. However, the policy does not describe the role of the CIO in enforcing these policies and procedures. For example, the policy does not describe a process for determining disciplinary action for employees that violate the policy and the role of the CIO in such a process. Thus, we did not change our assessment for this responsibility.

GSA's comments are reprinted in appendix XX.

- In an email on June 25, 2018, an OMB liaison stated that the agency agreed with two of our recommendations and partially agreed with the third recommendation. Specifically, the liaison

[79] See, e.g., GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Supersedes AIMD-10.1.23), GAO-04-394G (Washington, D.C.: March 2004) and SEI, *Capability Maturity Model® Integration for Acquisition (CMMI-ACQ)*, Version 1.3 (November 2010).

stated that OMB agrees with our recommendations to (1) update existing guidance to clearly explain how agencies are to address the role of CIOs to comply with the statutory requirements for CIOs to have a significant role in budgeting decisions and in the management, governance, and oversight processes related to IT; and (2) define the authority that CIOs are to have when agencies report on CIO authority over IT spending.

In addition, the OMB liaison stated that OMB partially agrees with the recommendation to issue guidance that addresses the 12 CIO responsibilities discussed in this report that are not included in existing OMB guidance. In particular, OMB stated that the agency concurs with issuing updated guidance to address CIO responsibilities that are not adequately included in existing guidance. However, the liaison stated that OMB believes that the following responsibilities are adequately included in existing OMB guidance.

- *Assume responsibility and accountability for IT investments.* OMB stated its implementation guidance for FITARA and related IT management practices—[80]specifically the common baseline section—describes how CIOs are to assume responsibility and accountability for IT investments. In particular, OMB cited the practices of the CIO (1) defining IT management processes and policies and (2) recommending modification, termination, or pause of IT projects or initiatives.

  Although we agree that effective implementation of these practices could help CIOs to assume responsibility and accountability for IT investments, OMB's implementation guidance for FITARA and related IT management practices does not explicitly address this responsibility. Until OMB issues guidance to address the role of the CIO for assuming responsibility and accountability for IT investments, CIOs may be limited in their abilities to fully implement this responsibility.

- *Coordinate with the agency head and chief financial officer to ensure that the financial systems are adequately implemented.* OMB stated its implementation guidance for FITARA and related IT management practices—specifically the common baseline section—describes how CIOs are to coordinate with the agency head and chief financial officer to ensure financial systems are adequately implemented. In particular, OMB cited the practices of

[80] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

the CIO to (1) establish and maintain a process to regularly engage with IT investment program managers; (2) define an agency-wide policy, in coordination with the chief financial officer and CAO, for the level of detail of planned expenditure reporting for all transactions that include IT resources; (3) define IT management processes and policies; and (4) be a member of governance boards that include IT resources, including bureau investment boards.

Although we agree that effective implementation of these practices could help CIOs to ensure that financial systems are adequately implemented, OMB's implementation guidance for FITARA and related IT management practices does not explicitly address this responsibility. Until OMB issues guidance to address the role of the CIO for coordinating with the agency head and chief financial offer to ensure that financial systems are adequately implemented, CIOs may be limited in their abilities to fully implement this responsibility.

- *Ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out their information security responsibilities.* OMB stated its Circular No. A-130, *Managing Information as a Strategic Resource* addresses this responsibility.[81]

  However, we reviewed OMB's Circular No. A-130 and this responsibility is not addressed in that policy. Until OMB updates its policy to address the role of the CIO for ensuring that senior agency officials carry out their information security responsibilities, CIOs may be limited in their abilities to fully implement this responsibility.

- *Ensure that all personnel are held accountable for complying with the agency-wide information security program*. OMB stated its Circular No. A-130, *Managing Information as a Strategic Resource* addresses this responsibility.

  However, we reviewed OMB's Circular No. A-130 and this responsibility is not addressed in that policy. Until OMB updates its policy to address the role of the CIO for ensuring that all personnel are held accountable for complying with the agency-

[81] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 28, 2016).

wide information security program, CIOs may be limited in their abilities to fully implement this responsibility.

Further, after we provided our draft report to OMB for comment, the President signed an executive order that, among other things, clarified the role that CIOs are to have on governance boards that review IT resources, including bureau investment review boards.[82] In particular, the executive order requires that the agency CIO be a member of any investment board with purview over IT, or any board responsible for setting agency-wide IT standards. Further, the order requires the head of each agency to direct the CIO to chair any such boards, as appropriate and consistent with applicable law.

This executive order is responsive to our recommendation for OMB to clearly explain how agencies are to address the role of CIOs to comply with the statutory requirements for CIOs to have a significant role in the management, governance, and oversight processes related to IT. We will monitor agencies' implementation of the executive order.

OMB also provided technical comments, which we have incorporated in the report, as appropriate.

- SBA agreed with most of our recommendation but had concerns with the following eight findings:
  - *Evaluate IT investments according to risk*. SBA believed that its policies require that each IT investment is reviewed utilizing a risk-based evaluation. However, SBA did not identify or provide such policies. Thus, we did not change our assessment for this responsibility.
  - *Report to the agency head or that official's deputy*. SBA stated that its CIO reports directly to the SBA Administrator and meets formally monthly to provide a status of all critical projects and activities. After we sent our draft report to the agency for comment, SBA provided us with an updated organizational structure showing that the CIO reports to the Administrator. Thus, we updated our assessment for this responsibility from not addressed to fully addressed.
  - *Review and approve IT budget requests*. SBA noted that it established a policy requiring all IT acquisitions greater than $50,000 to be reviewed and approved by the CIO prior to a

[82] Exec. Order No. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*; 83 Fed. Reg. 23345 (May 15, 2018).

solicitation being released. We agree that SBA's policy regarding the review of IT acquisitions fully addressed the role of the CIO in reviewing and approving IT contracts, acquisition plans, or strategies. However, this policy does not address the role of the CIO in reviewing and approving IT budget requests. Thus, we did not change our assessment for this responsibility.

- *Improve the management of the agency's IT portfolio through portfolio review (PortfolioStat)*: SBA explained that it uses several governance tools to review its IT portfolio. For example, the agency explained that the CIO meets quarterly with OMB for PortfolioStats. However, SBA did not provide a policy that addresses the role of its CIO for this responsibility. Thus, we did not change our assessment for this responsibility.
- *Evaluate IT investments according to risk (IT Dashboard CIO ratings)*. SBA stated that its CIO reviews all major IT investments on a monthly basis to evaluate IT investments for the OMB IT Dashboard CIO ratings. However, SBA did not provide a policy that addresses the role of its CIO for this responsibility. Thus, we did not change our assessment for this responsibility.
- *Review high-risk IT investments using TechStat sessions*: SBA correctly stated that we planned to change our assessment of this responsibility to "partially addressed" based on SBA's procedures for managing IT investments through its investment review board. However, as part of our subsequent review of these procedures, we determined that, although the procedures define TechStat reviews, the procedures do not describe the role of the CIO in conducting TechStat reviews. Thus, we did not change our assessment for this responsibility.
- *Maintain an inventory of data centers:* SBA stated that it maintains an inventory of data centers and can provide us with this information. Further, as part of our prior work on data center consolidation and optimization, we have recognized that SBA has developed an inventory of data centers.[83] However, SBA did not provide a policy that calls for the CIO to continue to maintain such an inventory. Thus, we did not change our assessment for this responsibility.

[83] See, e.g., GAO, *Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*, GAO-17-388 (Washington, D.C.: May 18, 2017).

- *Maintain a strategy to consolidate and optimize data centers*: SBA stated that it has a strategy regarding the consolidation and optimization of its data centers. SBA added that the document is located on the SBA website in accordance with the OMB requirement that SBA maintain and update its data center optimization strategy. In addition, as part of our prior work on data center consolidation and optimization, we have recognized that SBA has developed a strategy for consolidating and optimizing data centers.[84] However, SBA did not provide a policy that calls for the CIO to continue to maintain such a strategy. Thus, we did not change our assessment for this responsibility.

SBA's comments are reprinted in appendix XXI.

Further, one agency—NRC—disagreed with our recommendation. Specifically, NRC generally agreed with the findings, but did not agree with our recommendation related to IT leadership and accountability, workforce, and investment management.

- *Leadership and accountability*. NRC stated that it has fully addressed the requirement for the CIO to report directly to the agency head or that official's deputy. According to NRC, the agency's organizational legislation (*Reorganization Plan No. 1 of 1980*) assigns the agency's "administrative functions" to the Chairman and then requires the Chairman to delegate them to the Executive Director for Operations. NRC explained that the agency's CIO reports directly to the Executive Director for Operations, who serves as the Chief Operating Officer, and that the CIO has direct access to the Chairman. NRC further noted that this structure is also consistent with OMB's implementation guidance for FITARA and related IT management practices.[85]

Nevertheless, under law[86] and OMB guidance, agency CIOs must either report directly to the agency head or to the Deputy Secretary, unless agency-specific legislation calls for the CIO to report to an official other than the agency head. NRC's CIO does not report to the agency head and the agency's Executive Director for Operations does not have agency-wide authority comparable to a Deputy Secretary. In

[84] GAO-17-388.

[85] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[86] 44 U.S.C. § 3506(a)(2)(A).

addition, NRC's organizational legislation neither overrides the current statutory requirement for the CIO to report to the agency head nor does it assign the statutory IT management responsibilities to another official. Thus, we did not change our assessment for this responsibility.

- *IT workforce*. NRC believed that it partially addressed the responsibilities to (1) assess annually the requirements established for agency personnel regarding IT management knowledge and skills, (2) assess annually the extent to which agency personnel meet IT management knowledge and skill requirements, and (3) annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies.

Regarding the first responsibility, NRC indicated that its C*apital Planning and Investment Control Policy and Overview* calls for the CIO and Chief Human Capital Officer to develop a set of competency requirements for IT and acquisition staff. In addition, NRC stated that it recently reissued *MD 12.5, NRC Cyber Security Program* to specifically define these CIO responsibilities.

We agree that the *Capital Planning and Investment Control Policy and Overview* and cybersecurity program directive partially address assessing the requirements for IT management and skill gaps. However, those policies do not call for the CIO to conduct the assessment on an annual basis. Thus, we updated our assessment for this responsibility from not addressed to partially addressed.

Regarding the second responsibility, NRC noted that its *Capital Planning and Investment Control Policy and Overview* calls for the CIO and Chief Human Capital Officer to develop a set of competency requirements for IT and acquisition staff and to develop and maintain a current workforce planning process. In addition, NRC stated that it recently reissued *MD 12.5, NRC Cyber Security Program*, to specifically define these CIO responsibilities.

Both of the policies call for the CIO to develop a workforce planning process. However, the policies do not call for that process to include annually assessing the extent to which agency personnel meet IT management knowledge and skill requirements. Thus, we did not change our assessment for this responsibility.

With respect to the third responsibility, NRC stated that *MD 10.1 Recruitment, Appointments, and Merit Staffing* and *MD 10.77 Employee Development and Training* require all NRC Office Directors, including the CIO, to work with the Chief Human Capital Officer to annually build a staffing plan and a prioritized list of training for their staff. NRC's policies on recruitment, staffing, and training call for the CIO to annually build a staffing plan and a prioritized list of training.

Both of the policies call for the CIO to build a staffing plan and list of training. However, these policies do not call for the CIO to develop such a plan in order to address knowledge and skill deficiencies as identified in a skill gap assessment. Thus, we did not change our assessment for this responsibility.

- *IT investment management*. NRC maintained that it fully addressed the responsibility for the CIO to maintain a strategy to consolidate and optimize data centers. According to NRC, it maintains and posts its *Data Center Optimization Initiative Strategic Plan* on its public website. In addition, NRC provided a certification memorandum from the CIO to the Federal CIO and posted it on NRC's public website.

However, these documents do not call for the CIO to maintain a strategy to consolidate and optimize data centers. Developing such a policy is important to ensure that NRC continues to develop and implement a strategy for consolidating and optimizing data centers. Thus, we did not change our assessment for this responsibility.

NRC's comments are reprinted in appendix XXII.

Lastly, five agencies did not state whether they agreed or disagreed with our recommendations although two of them offered other comments:

- HUD stated that it had reviewed the draft report and did not have any comments. HUD's statement is reprinted in appendix XXIII.
- In emails received from Labor and Treasury, the agencies did not agree or disagree with our recommendations and did not have any other comments on the report.
- EPA neither agreed nor disagreed with our recommendation and stated that it agrees in principle that CIO authorities should be adequately documented in appropriate policies. According to the agency, our engagement documents a large number of CIO authorities that are not yet captured in policy documents. EPA explained that some of the responsibilities lack policy or other supporting processes, while other responsibilities have supporting processes in place and simply require a policy statement to formalize the authority. In addition, EPA stated that some responsibilities require an assessment as to whether the agency is positioned—either from a resource or process ownership perspective—to implement a policy.

EPA further explained that it intends to determine which of the responsibilities identified in our report are on the agency's fiscal year 2018 agenda for documenting IT policy items, and which of them should be included on the agency's fiscal year 2019 agenda.

EPA's comments are reprinted in appendix XXIV.

- USAID did not comment on our recommendation to the agency. USAID added that it is committed to fully complying with the requirements of FISMA 2014 and FITARA, and it views the statutory mandates as integral components of its risk management framework. USAID stated that it has made significant improvements in its IT policies and processes since we completed our work. Further, USAID provided the three following comments.

  - First, USAID believes that many of the deficiencies identified in the report are better characterized as gaps in documentation, as the agency's CIO is already performing the key responsibilities. USAID said that, while the agency may not have yet published policies that fully describe the role of the CIO for all responsibilities, the CIO is performing nearly all of the key responsibilities identified in our report. USAID noted that it is revising a chapter of its policy manual.

    We recognize that some CIOs are implementing these responsibilities in the absence of policies. However, as we previously stated, the 24 CIOs that we surveyed noted that they were not always very effective in implementing the six IT management areas. Correspondingly, the two areas in which CIOs stated they were least effective—IT strategic planning and IT workforce—were the same two areas for which the majority of the agencies minimally addressed or did not address the role of their CIOs. As such, developing policies that address the role of the CIO for key responsibilities would increase the likelihood that these responsibilities are implemented effectively. Moreover, establishing policies would better position future USAID CIOs.

  - Second, USAID stated that it has addressed seven of the responsibilities that we identified as not fully addressed. In addition, USAID plans to fully address an additional eight responsibilities in the coming months with the publication of its new policy on implementing FITARA. Further, USAID is updating its policies to address six of the responsibilities that we identified as not addressed. As an example, USAID stated that the agency's

  - transformation plan will propose making the CIO a direct report to the Administrator.

    We have not yet reviewed the actions that USAID has taken to fully address the key CIO responsibilities. If the agency follows through on its plans to ensure that its policies fully address the role of its CIO, that official should be better positioned to effectively carry out key IT management responsibilities.
  - Third, USAID agreed that additional guidance from OMB to clearly define CIOs' authorities would assist USAID's efforts to consolidate its IT planning, budgeting, and programming.

  USAID's comments are reprinted in appendix XXV.

We are sending 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, the report will be available at no charge on GAO's website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact David A. Powner at (202) 512-9286 or pownerd@gao.gov, or Carol C. Harris at (202) 512-4456 or harriscc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix XXVI.

David a. Po

David A. Powner
Director, Information Technology Management Issues

CCHarris

Carol C. Harris
Director, Information Technology Acquisition Management Issues

*List of Requesters*

The Honorable Trey Gowdy
Chairman
The Honorable Elijah Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Mark Meadows
Chairman
The Honorable Gerald E. Connolly
Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Government Reform
House of Representatives

The Honorable Will Hurd
Chairman
The Honorable Robin L. Kelly
Ranking Member
Subcommittee on Information Technology
Committee on Oversight and Government Reform
House of Representatives

# Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the extent to which agencies have addressed the role of the Chief Information Officer (CIO) in accordance with federal laws and guidance, and (2) describe major factors that have enabled and challenged agency CIOs in fulfilling their responsibilities to carry out federal laws and guidance. The scope of our review included the 24 agencies covered by the Chief Financial Officers Act of 1990.[1]

To determine the extent to which agencies have addressed the role of the CIO in accordance with federal laws and guidance, we created an evaluation framework, assessed the information technology (IT) management policies of selected agencies against the evaluation framework, assessed the extent to which the Office of Management and Budget's (OMB) guidance comprehensively and clearly addressed the responsibilities in the evaluation framework, and surveyed CIOs on how effective they have been in carrying out their key IT management responsibilities.

To create the evaluation framework, we reviewed relevant laws to identify key IT management responsibilities of federal CIOs.[2] In particular, we reviewed relevant provisions of the following laws:

- *Paperwork Reduction Act of 1980,*[3]
- *Paperwork Reduction Reauthorization Act of 1986,*[4]

[1] 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.

[2] We did not review the following CIO responsibilities relating to information management: information collection/paperwork reduction, information dissemination, information disclosure, statistical policy and coordination, records management, and privacy.

[3] Pub. L. No. 96-511 (Dec. 11, 1980).

- *Paperwork Reduction Act of 1995,*[5]
- *Clinger-Cohen Act of 1996,*[6]
- *Federal Information Security Management Act of 2002* (FISMA 2002),[7]
- *Legislation commonly referred to as the Federal Information Technology Acquisition Reform Act* (FITARA),[8] *and*
- *Federal Information Security Modernization Act of 2014* (FISMA 2014)*.*[9]

We also reviewed key requirements in OMB guidance on agency CIO IT management and information security responsibilities. In particular, we reviewed

- *Managing Information as a Strategic Resource*, Circular No. A-130,[10] and
- *Management and Oversight of Federal Information Technology, Memorandum* M-15-14.[11]

Based on our review of the laws and guidance, we identified 35 key CIO IT management responsibilities and categorized them in six IT

[4] Pub. L. No. 99-591, Title VIII (Oct. 30, 1986).

[5] Pub. L. No. 104-13 (May 22, 1995); 44 U.S.C. §§ 3501-3521.

[6] Pub. L. No. 104-106, Div. E, (Feb. 10, 1996). The law, initially titled the Information Technology Management Reform Act, was subsequently renamed the Clinger-Cohen Act in P.L. 104-208, (Sept. 30, 1996); 40 U.S.C. §§ 11101-11703.

[7] Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2946 (Dec. 17, 2002). FISMA 2002's amendments to title 44, U.S. Code, were superseded by the enactment of FISMA 2014. However, FISMA 2002's amendments to sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. §§ 278g-3 and g-4), regarding NIST standards and guidance, continue in effect.

[8] 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).

[9] Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014); 44 U.S.C. §§ 3551-3558.

[10] OMB, Circular No. A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 28, 2016).

[11] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

management areas. Those areas and the associated responsibilities are shown in table 2.

Table 2: Summary of Key Chief Information Officer (CIO) Responsibilities

| Responsibility | Source |
|---|---|
| **Information technology (IT) leadership and accountability** – *CIOs are responsible and accountable for the effective implementation of IT management responsibilities.* | |
| Report directly to the agency head or that official's deputy.[a] | *44 USC § 3506 (a)(2)(A) and OMB M-15-14* |
| Assume responsibility and accountability for IT investments. | *44 USC § 3506(h)(2)* and 40 USC § 11312 |
| Approve the selection of bureau CIOs. | *40 U.S.C. § 11319(b)(2), OMB A-130, and OMB M-15-14* |
| Provide input into bureau CIO performance evaluations. | *40 U.S.C. § 11315(c)(3)(B), OMB A-130, and OMB M-15-14* |
| Designate a senior agency information security officer. | *44 U.S.C. § 3554(a)(3)(A)* |
| **IT strategic planning** – *CIOs are responsible for strategic planning for all IT management functions.* | |
| Establish goals for improving agency operations through IT. | *40 U.S.C. § 11313 (1)* |
| Measure how well IT supports agency programs. | *40 U.S.C. § 11313 (3)* |
| Prepare an annual report on the progress in achieving the goals. | *40 U.S.C. § 11313 (2)* |
| Benchmark agency processes against private and public sector performance. | *40 U.S.C. § 11313 (4)* |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments. | *40 U.S.C. § 11313 (5)* |
| **IT workforce** – *CIOs are responsible for assessing agency IT workforce needs and developing strategies and plans for meeting those needs.* | |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills. | *40 U.S.C. § 11315(c)(3)(A), OMB A-130, and OMB M-15-14* |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements. | *40 U.S.C. § 11315(c)(3)(B)* |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies. | *40 U.S.C. § 11315(c)(3)(C)* |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities. | *40 U.S.C. § 11315(c)(3)(D)* |
| **IT budgeting** – *CIOs are responsible for the processes for all annual and multi-year IT planning, programming, and budgeting decisions.* | |
| Have a significant role in IT planning, programming, and budgeting decisions. | *40 U.S.C. § 11319 (b)(1)(A), OMB A-130, and OMB M-15-14* |
| Ensure that the agency implements a process for selecting IT investments. | *44 U.S.C. § 3506 (h)(5)(B) and 40 USC § 11312(b)(1)* |
| Review and approve the IT budget request. | *40 U.S.C. § 11319 (b)(1)(B)(i) and OMB M-15-14* |
| Review and approve funding reprogramming requests (i.e., shifting funds within an appropriation fund or account). | *40 U.S.C. § 11319 (b)(1)(C)(i)(II) and OMB M-15-14* |
| **IT investment management** – *CIOs are responsible for the processes for managing, evaluating, and assessing how well the agency is managing its IT resources.* | |

| Responsibility | Source |
|---|---|
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT. | *40 U.S.C. § 11319(b)(1)(A), 40 U.S.C. § 11315, 44 U.S.C. § 3506(a), OMB A-130, and OMB M-15-14* |
| Improve the management of the agency's IT through portfolio review (PortfolioStat). | *40 U.S.C. § 11319(d)(1)&(2) and OMB M-15-14* |
| Ensure that the agency implements a process for controlling and evaluating IT investments. | *44 USC 3506(h)(5)(b) and 40 U.S.C. §§ 11312 & 11313* |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings). | *40 U.S.C. § 11302 and OMB M-15-14* |
| Review high-risk IT investments (TechStat sessions). | *40 U.S.C. § 11302(c)(4), OMB A-130, and OMB M-15-14* |
| Certify that investments are adequately implementing incremental development consistent with Office of Management and Budget (OMB) capital planning guidance. | *40 U.S.C § 11319(b)(1)(B)(ii) and OMB M-15-14* |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation. | *40 U.S.C. § 11315(c)(2) and OMB M-15-14* |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented. | *40 U.S.C. 11316* |
| Review and approve IT contracts, acquisition plans, or strategies.[b] | *40 U.S.C. § 11319(b)(1)(C)(i)(I), OMB A-130, and OMB M-15-14* |
| Maintain an inventory of data centers. | *44 U.S.C. § 3601 note* |
| Maintain a strategy to consolidate and optimize data centers. | *44 U.S.C. § 3601 note* |
| **Information security** – *CIOs are responsible for establishing, implementing, and ensuring compliance with an agency-wide information security program.* | |
| Develop and maintain an agency-wide information security program. | *44 U.S.C. § 3554(a)(3)(B)* |
| Develop and maintain information security policies, procedures, and control techniques. | *44 U.S.C. § 3554(a)(3)* |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities. | *44 U.S.C. § 3554(a)(6)* |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques. | *44 U.S.C. § 3554(a)(4) and 44 U.S.C. § 3554(a)(3)(D)* |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program. | *44 U.S.C. § 3554(a)(7)* |
| Report annually to the agency head on the effectiveness of the agency information security program. | *44 U.S.C. § 3554(a)(5)* |

Source: GAO analysis of federal legislation and guidance. | GAO-18-93

[a] The law requires the CIO to report directly to the agency head and OMB's implementing guidance states that CIOs may report to the head of the agency (e.g., secretary) or that official's deputy (e.g., deputy secretary) who acts on behalf of the agency's overall leader.

[b] The law requires CIOs to review and approve IT contracts and OMB's implementing guidance states that CIOs may review and approve IT acquisition strategies and plans, rather than individual IT contracts.

We then assessed the selected agencies' IT management documents against the framework. To do so, we first collected IT management policies and procedures, agency organizational structures, CIO position descriptions, as well as agency submissions to OMB regarding CIO involvement in IT governance boards. We also reviewed our prior work on (1) CIO review of acquisition plans and strategies,[12] (2) CIO certification of incremental development,[13] and (3) the Department of Homeland Security implementation of FITARA,[14] as well as agencies' efforts to address our related recommendations. We then evaluated the agencies' documents to determine whether they addressed the role of the CIO consistent with the key responsibilities found in our framework. We assessed each responsibility as:

- *fully addressed*—the agency provided evidence that described the CIO's role for carrying out the responsibility;
- *partially addressed*—the agency provided evidence that described the CIO's role for about half or a large portion of the responsibility; or
- *not addressed*—the agency did not provide evidence that described the CIO's role for carrying out the responsibility.

We also summarized the results of these assessments for each of the six areas. Specifically, we assessed each area as:

- *fully addressed*—the agency provided evidence that described the CIO's role for carrying out all of the related responsibilities;
- *substantially addressed*—the agency provided evidence that described the CIO's role for at least two-thirds, but not all, of the related responsibilities;
- *partially addressed*—the agency provided evidence that described the CIO's role for at least one-third, but less than two-thirds, of the related responsibilities;
- *minimally addressed*—the agency provided evidence that described the CIO's role for less than one-third of the related responsibilities; or

[12] GAO, *Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions*, GAO-18-42 (Washington, D.C.: Jan. 10, 2018).

[13] GAO, *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development*, GAO-18-148 (Washington, D.C.: Nov. 7, 2017).

[14] GAO, *Homeland Security: Progress Made to Implement IT Reform, but Additional Chief Information Officer Involvement Needed*, GAO-17-284 (Washington, D.C.: May 18, 2017).

- *not addressed*—the agency did not provide evidence that described the CIO's role for carrying out any of the related responsibilities.

Further, to assess the extent to which OMB's guidance addressed the responsibilities in the evaluation framework, we interviewed officials from OMB to obtain information about the agency's guidance on IT management responsibilities of CIOs. We then assessed the extent to which OMB's guidance addressed the responsibilities in the evaluation framework.

To obtain CIOs' views on how effective they have been in carrying out the responsibilities identified in our evaluation framework, we administered a survey to the CIOs of each of the 24 agencies. We designed the survey questions in collaboration with a survey specialist, incorporated technical feedback from a separate survey specialist, and pretested the questions with officials at five agencies. We then made revisions as necessary to reduce the likelihood of overall and item non-response, as well as reporting errors on our questions. We sent the survey to the CIOs via email on December 15, 2016, and closed the survey on February 14, 2017. We received a completed survey response from the CIOs of 23 of the 24 selected agencies. The survey response for the 1 remaining agency, the Department of Defense, was completed by the Deputy CIO.[15]

Survey data were electronically extracted and analyzed using a statistical program. We examined the survey results and performed computer analyses to identify missing data, inconsistencies, and other indications of error, and addressed such issues as necessary, including through follow-up communications with the CIOs. Quantitative data analyses were conducted by a GAO survey specialist and a review of open-ended responses was conducted by the GAO staff with subject matter expertise. An independent GAO data analyst checked the statistical computer program for accuracy.

Because we surveyed all of the CIOs and, therefore, did not conduct any sampling for our survey, our data are not subject to sampling errors. However, the practical difficulties of conducting any survey may introduce non-sampling errors. For example, errors can be introduced into the results due to differences in how a particular question is interpreted, the

[15] For reporting purposes, when referring to the survey data as being from CIOs, we are including the Deputy CIO.

sources of information available to respondents, or the types of people who do not respond to a question. We included steps in both the data collection and data analysis stages to minimize such non-sampling errors.

In the survey, we asked the CIOs to identify how effective they have been in carrying out their key IT management responsibilities since December 2014, when FITARA was enacted. To obtain additional narrative and supporting context, we then interviewed 22 CIOs and 1 Deputy CIO.[16]

To address our second objective, as part of the previously mentioned survey, we asked CIOs to describe the extent to which certain factors have enabled or challenged their ability to effectively carry out their key IT management responsibilities since December 2014, when FITARA was enacted. In the survey, we identified 25 potential factors that could enable or challenge the CIOs' ability to effectively manage IT.[17] We asked the CIOs to rate whether each factor was a minor enabler, major enabler, minor challenge, major challenge, or neither enabling nor challenging. We then totaled the number of times each factor was identified by CIOs, choosing to report on the factors that were identified by at least half of the CIOs.

We also evaluated the efforts of OMB's Office of E-Government and Information Technology address factors that challenged CIOs' ability to effectively carry out their responsibilities, including OMB's call for agencies to provide data on CIO authority over planned IT spending. Further, we collected and analyzed information on the tenure of the 24 agencies' current and former CIOs.[18]

To determine the reliability of the data on CIO authority over planned IT spending, we asked agency officials to verify the accuracy and completeness of these data and provide the correct information where needed. We also reviewed these data for obvious errors in accuracy and completeness and obtained clarification from agencies on identified

[16] The Department of Defense CIO declined to meet with us and the Department of Homeland Security made the Deputy CIO available for an interview, in lieu of the CIO.

[17] To develop the list of 25 factors, we reviewed our prior work on enabling and challenging factors for Chief Information Security Officers and discussed the list with internal subject matter experts. We also discussed these factors with officials at five agencies as part of our survey pretest to ensure that the list of factors was complete.

[18] We collected information on individuals that filled the role of the 24 CIOs between January 1, 2004, and November 30, 2017.

errors. We determined that the data were sufficiently reliable for the purpose of this report, which was to describe reported levels of CIO authority over IT spending, in aggregate form, and agency definitions of CIO authority over IT spending.

We conducted this performance audit from August 2016 to August 2018 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: CIO Tenure

Tables 3 and 4 present analysis related to the tenure of CIOs at each of the 24 Chief Financial Officers Act agencies from 2004 to 2017.

Table 3: Analysis of Chief Information Officer (CIO) Tenure (2004-2017)

| | Permanent and acting CIOs, including current CIOs | Permanent and acting CIOs, excluding current CIOs | Permanent CIOs, including current CIOs | Permanent CIOs, excluding current CIOs |
|---|---|---|---|---|
| Number of CIOs in this population | 191 | 167 | 114 | 98 |
| Mean | 1.9 | 2.0 | 2.8 | 3.0 |
| Median | 1.5 | 1.5 | 2.3 | 2.5 |
| Number of CIOs in office at least 3 years | 43 | 40 | 43 | 40 |
| Percentage of CIOs in office at least 3 years | 23 | 24 | 38 | 41 |

Source: GAO analysis of data from 24 Chief Financial Officers Act agencies on the tenure of their CIOs. | GAO-18-93

Note: This describes the tenure of CIOs who were in office between January 1, 2004, and November 30, 2017. We reflected the full tenure of CIOs who were in that position on January 1, 2004, including their service prior to that date. In addition, CIOs who moved from acting to permanent status have been treated as if they were permanent the entire time, and calculations were performed on their aggregated time as one length of service.

Table 4: Analysis of Chief Information Officer (CIO) Tenure (2012-2017)

| | Permanent and acting CIOs, including current CIOs | Permanent and acting CIOs, excluding current CIOs | Permanent CIOs, including current CIOs | Permanent CIOs, excluding current CIOs |
|---|---|---|---|---|
| Number of CIOs in this population | 101 | 77 | 62 | 46 |
| Mean | 1.9 | 2.1 | 2.7 | 3.1 |
| Median | 1.5 | 1.7 | 2.2 | 2.7 |
| Number of CIOs in office at least 3 years | 25 | 22 | 25 | 22 |
| Percentage of CIOs in office at least 3 years | 25 | 29 | 40 | 48 |

Source: GAO analysis of data from 24 Chief Financial Officers Act agencies on the tenure of their CIOs. | GAO-18-93

Note: This describes the tenure of CIOs who were in office between January 1, 2012, and November 30, 2017. We reflected the full tenure of CIOs who were in that position on January 1, 2012, including their service prior to that date. In addition, CIOs who moved from acting to permanent status have been treated as if they were permanent the entire time, and calculations were performed on their aggregated time as one length of service.

# Appendix III: Assessment of the Extent to Which Agencies' Policies Addressed the Role of Their CIOs, Arranged by Agency

This appendix contains the profiles for the 24 Chief Financial Officers Act agencies included in this review. The tables provide additional detail on areas in our Chief Information Officer (CIO) responsibility evaluation framework and our assessment of the extent to which the policies of each agency addressed each of the six areas and the 35 responsibilities that comprise them.

The following information describes the key that we used in the tables to convey the results of our assessment of each of the 35 responsibilities:

**Full Evidence (FE)**—the agency provided evidence that described the CIO's role for carrying out the responsibility

**Partial Evidence (PE)**—the agency provided evidence that described the CIO's role for about half or a large portion of the responsibility

**No Evidence (NE)**—the agency did not provide evidence that described the CIO's role for carrying out the responsibility

Further, the following information describes the key that we used in the tables to convey the results of our assessment of each of the six areas:

Fully—the agency provided evidence that described the CIO's role for carrying out all of the related responsibilities

Substantially—the agency provided evidence that described the CIO's role for at least two-thirds, but not all, of the related responsibilities

Partially—the agency provided evidence that described the CIO's role for at least one-third, but less than two-thirds, of the related responsibilities

Minimally—the agency provided evidence that described the CIO's role for less than one-third of the related responsibilities

Not at all—the agency did not provide evidence that described the CIO's role for carrying out the any of the related responsibilities

## Department of Agriculture

**Department of Agriculture**

**Fiscal year 2018 information technology (IT) funding request**: $2,958 million

**Development**: $418 million

**Operations and maintenance**: $2,540 million

**Official to whom the Chief Information Officer (CIO) reports**: Assistant Secretary for Administration

**CIO appointment type**: Career

**Status of current CIO**: Acting

**Number of CIOs since 2004**: 9

**Number of CIOs since 2012**: 6

**Average tenure of CIOs (not including the current CIO) since 2004**: 1.8 years

**Average tenure of CIOs (not including the current CIO) since 2012**: 1.7 years

**Median tenure of CIOs (not including the current CIO) since 2004**: 2.0 years

**Median tenure of CIOs (not including the current CIO) since 2012**: 2.2 years

**Tenure of current CIO**: 2 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 5: Extent to Which Department of Agriculture Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Partially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | NE |
| Designate a senior agency information security officer | NE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Partially** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | FE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | PE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | PE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Agriculture policies. | GAO-18-93

## Department of Commerce

**Department of Commerce**

**Fiscal year 2018 information technology (IT) funding request**: $2,555 million

**Development:** $904 million

**Operations and maintenance**: $1,651 million

**Official to whom the Chief Information Officer (CIO) reports**: Deputy Secretary

**CIO appointment type**: Appointment

**Status of current CIO**: Acting

**Number of CIOs since 2004**: 7

**Number of CIOs since 2012:** 3

**Average tenure of CIOs (not including the current CIO) since 2004**: 2.5 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 3.3 years

**Median tenure of CIOs (not including the current CIO) since 2004**: 2.5 years

**Median tenure of CIOs (not including the current CIO) since 2012**: 3.3 years

**Tenure of current CIO**: 11 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 6: Extent to Which Department of Commerce Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Minimally** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | FE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | FE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | PE |

Source: GAO analysis of Department of Commerce policies. | GAO-18-93

## Department of Defense

**Department of Defense**

**Fiscal year 2018 information technology (IT) funding request:** $42,500 million

**Development**: $10,500 million

**Operations and maintenance**: $31,978 million

**Official to whom the Chief Information Officer (CIO) reports:** Secretary

**CIO appointment type**: Career

**Status of current CIO:** Acting

**Number of CIOs since 2004**: 8

**Number of CIOs since 2012**: 4

**Average tenure of CIOs (not including the current CIO) since 2004**: 2 years

**Average tenure of CIOs (not including the current CIO) since 2012**: 2.1 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.7 years

**Median tenure of CIOs (not including the current CIO) since 2012**: 2.8 years

**Tenure of current CIO**: 10 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 7: Extent to Which Department of Defense Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | NE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | FE |
| **IT Workforce** | **Partially** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | PE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | PE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Fully** |
| Have a significant role in IT planning, programming, and budgeting decisions | N/A |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | N/A |
| **IT Investment Management** | **Substantially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | N/A |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | FE |
| Review and approve IT contracts, acquisition plans, or strategies | N/A |
| Maintain an inventory of data centers | FE |
| Maintain a strategy to consolidate and optimize data centers | FE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | FE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | FE |
| Report annually to the agency head on the effectiveness of the agency information security program | PE |

Source: GAO analysis of Department of Defense policies. | GAO-18-93

## Department of Education

**Department of Education**

**Fiscal year 2018 information technology (IT) funding request:** $745 million

**Development:** $125 million

**Operations and maintenance:** $619 million

**Official to whom the Chief Information Officer (CIO) reports:** Deputy Secretary

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 5

**Number of CIOS since 2012:** 2

**Average tenure of CIOs (not including the current CIO) since 2004:** 3.5 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 7.4 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 2.8 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 7.4 years

**Tenure of current CIO:** 1.5 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 8: Extent to Which Department of Education Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Substantially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | N/A |
| Maintain a strategy to consolidate and optimize data centers | N/A |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of Department of Education policies. | GAO-18-93

## Department of Energy

**Department of Energy**

**Fiscal year 2018 information technology (IT) funding request:** $1,850 million

**Development:** $166 million

**Operations and maintenance**: $1,685 million

**Official to whom the Chief Information Officer (CIO) reports:** Secretary

**CIO appointment type:** Appointment

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 9

**Number of CIOs since 2012:** 6

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.7 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.3 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.6 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 1.5 years

**Tenure of current CIO:** 5 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 9: Extent to Which Department of Energy Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | PE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | PE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | FE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | FE |
| Review and approve IT contracts, acquisition plans, or strategies | NE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | PE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Energy policies. | GAO-18-93

## Department of Health and Human Services

**Department of Health and Human Services**

**Fiscal year 2018 information technology (IT) funding request:** $13,833 million

**Development:** $3,680 million

**Operations and maintenance:** $10,153 million

**Official to whom the Chief Information Officer (CIO) reports:** Assistant Secretary for Administration

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 7

**Number of CIOs since 2012:** 3

**Average tenure of CIOs (not including the current CIO) since 2004:** 2.0 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 2.2 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.9 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 2.2 years

**Tenure of current CIO:** 2.0 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 10: Extent to Which Department of Health and Human Services Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Partially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | NE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Minimally** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | PE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | PE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Health and Human Services policies. | GAO-18-93

## Department of Homeland Security

**Department of Homeland Security**

**Fiscal year 2018 information technology (IT) funding request:** $6,833 million

**Development:** $1,177 million

**Operations and maintenance:** $5,656 million

**Official to whom the Chief Information Officer (CIO) reports:** Undersecretary for Management

**CIO appointment type:** Presidential appointment

**Status of current CIO:** Acting

**Number of CIOs since 2004**: 12

Number of CIOs since 2012: 6

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.3 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.6 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 7 months

**Median tenure of CIOs (not including the current CIO) since 2012:** 7 months

**Tenure of current CIO:** 2 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 11: Extent to Which Department of Homeland Security Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Partially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | NE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Fully** |
| Have a significant role in IT planning, programming, and budgeting decisions | FE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | PE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | FE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | PE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | PE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Homeland Security policies. | GAO-18-93

## Department of Housing and Urban Development

**Department of Housing and Urban Development**

**Fiscal year 2018 information technology (IT) funding request:** $351 million

**Development:** $16 million

**Operations and maintenance:** $335 million

**Official to whom the Chief Information Officer (CIO) reports:** Chief Operations Officer

**CIO appointment type:** Appointment

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 13

**Number of CIOs since 2012:** 6

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.1 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.4 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 6 months

**Median tenure of CIOs (not including the current CIO) since 2012:** 5 months

**Tenure of current CIO:** 6 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 12: Extent to Which Department of Housing and Urban Development Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Partially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | NE |
| Provide input into bureau CIO performance evaluations | NE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | FE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |
| Ensure that the agency implements a process for controlling and evaluating IT investments | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | N/A |
| Maintain a strategy to consolidate and optimize data centers | N/A |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | NE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of Department of Housing and Urban Development policies. | GAO-18-93

## Department of the Interior

**Department of the Interior**

**Fiscal year 2018 information technology (IT) funding request:** $1,185 million

**Development:** $103 million

**Operations and maintenance:** $1,082 million

**Official to whom the Chief Information Officer (CIO) reports:** Secretary

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 8

**Number of CIOs since 2012:** 2

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.6 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 3.8 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.3 years

**Median tenure of CIOs (not including the current CIO) since 2012**: 3.8 years

**Tenure of current CIO:** 3.7 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 13: Extent to Which Department of the Interior Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Minimally** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | PE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | FE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of Department of the Interior policies. | GAO-18-93

## Department of Justice

**Department of Justice**

**Fiscal year 2018 information technology (IT) funding request:** $2,852 million

**Development:** $607 million

**Operations and maintenance:** $2,245 million

**Official to whom the Chief Information Officer (CIO) reports:** Assistant Attorney General for Administration

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 5

**Number of CIOs since 2012:** 4

**Average tenure of CIOs (not including the current CIO) since 2004:** 3 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 11 months

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.2 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 8 months

**Tenure of current CIO:** 3.5 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 14: Extent to Which Department of Justice Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Substantially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | FE |
| Benchmark agency processes against private and public sector performance | PE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Partially** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | PE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | PE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | FE |
| Ensure that the agency implements a process for selecting IT investments | PE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | FE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Fully** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | FE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | FE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Justice policies. | GAO-18-93

## Department of Labor

**Department of Labor**

**Fiscal year 2018 information technology (IT) funding request:** $703 million

**Development:** $111 million

**Operations and maintenance:** $592 million

**Official to whom the Chief Information Officer (CIO) reports:** Assistant Secretary for Administration and Management

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 5

**Number of CIOs since 2012:** 3

**Average tenure of CIOs (not including the current CIO) since 2004:** 3.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 3.7 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 3.7 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 3.7 years

**Tenure of current CIO:** 1.2 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 15: Extent to Which Department of Labor Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | FE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Substantially** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | FE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | FE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | FE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | PE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | PE |

Source: GAO analysis of Department of Labor policies. | GAO-18-93

## Department of State

**Department of State**

**Fiscal year 2018 information technology (IT) funding request:** $1,864 million

**Development:** $366 million

**Operations and maintenance:** $1,498 million

**Official to whom the Chief Information Officer (CIO) reports:** Undersecretary for Management

**CIO appointment type**: Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 10

**Number of CIOs since 2012:** 3

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.5 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 4.2 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 10 months

**Median tenure of CIOs (not including the current CIO) since 2012:** 4.2 years

**Tenure of current CIO:** 1.5 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 16: Extent to Which Department of State Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Partially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | NE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Minimally** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | PE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | NE |
| Maintain an inventory of data centers | FE |
| Maintain a strategy to consolidate and optimize data centers | FE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of Department of State policies. | GAO-18-93

## Department of Transportation

**Department of Transportation**

**Fiscal year 2018 information technology (IT) funding request:** $3,147 million

**Development:** $1,657 million

**Operations and maintenance:** $1,490 million

**Official to whom the Chief Information Officer (CIO) reports:** Deputy Secretary

**CIO appointment type:** Appointment

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 9

**Number of CIOs since 2012:** 5

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 2.1 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.7 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 2.0 years

**Tenure of current CIO:** 1 month

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 17: Extent to Which Department of Transportation Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Partially** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | FE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | PE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | NE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | FE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | PE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Transportation policies. | GAO-18-93

## Department of the Treasury

**Department of the Treasury**

**Fiscal year 2018 information technology (IT) funding request:** $4,182 million

**Development:** $631 million

**Operations and maintenance:** $3,551 million

**Official to whom the Chief Information Officer (CIO) reports:** Assistant Secretary for Management

**CIO appointment type:** Career

**Status of current CIO:** Acting

**Number of CIOs since 2004:** 11

**Number of CIOs since 2012:** 5

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.4 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.6 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 11 months

**Median tenure of CIOs (not including the current CIO) since 2012:** 1.5 years

**Tenure of current CIO:** 5 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 18: Extent to Which Department of the Treasury Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Partially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | NE |
| Provide input into bureau CIO performance evaluations | NE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Minimally** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | NE |
| Review and approve the IT budget request | PE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | NE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | PE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of Department of the Treasury policies. | GAO-18-93

## Department of Veterans Affairs

**Department of Veterans Affairs**

**Fiscal year 2018 information technology (IT) funding request:** $4,151 million

**Development:** $529 million

**Operations and maintenance:** $3,621 million

**Official to whom the Chief Information Officer (CIO) reports:** Deputy Secretary

**CIO appointment type:** Presidential appointment with Senate confirmation

**Status of current CIO:** Executive-in-charge

**Number of CIOs since 2004:** 9

Number of CIOs since 2012: 5

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 2.1 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.9 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 1.9 years

**Tenure of current CIO:** 2 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 19: Extent to Which Department of Veterans Affairs Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | NE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | NE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Fully** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | FE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | FE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Department of Veterans Affairs policies. | GAO-18-93

## Environmental Protection Agency

**Environmental Protection Agency**

**Fiscal year 2018 information technology (IT) funding request:** $328 million

**Development:** $32 million

**Operations and maintenance:** $296 million

**Official to whom the Chief Information Officer (CIO) reports:** Deputy Administrator

**CIO appointment type:** Appointment

**Status of current CIO:** Acting

**Number of CIOs since 2004:** 8

**Number of CIOs since 2012:** 4

**Average tenure of CIOs (not including the current CIO) since 2004:** 2.2 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 2.2 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.9 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 1.9 years

**Tenure of current CIO:** 11 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 20: Extent to Which Environmental Protection Agency Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | NE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Minimally** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | FE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Environmental Protection Agency policies. | GAO-18-93

## General Services Administration

**General Services Administration**

**Fiscal year 2018 information technology (IT) funding request:** $691 million

**Development:** $197 million

**Operations and maintenance:** $494 million

**Official to whom the Chief Information Officer (CIO) reports:** Deputy Administrator

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 4

**Number of CIO since 2012:** 3

**Average tenure of CIOs (not including the current CIO) since 2004:** 4.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 3.9 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 6.5 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 3.9 years

**Tenure of current CIO:** 2.7 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 21: Extent to Which General Services Administration Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Minimally** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Minimally** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | FE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of General Services Administration policies. | GAO-18-93

## National Aeronautics and Space Administration

**National Aeronautics and Space Administration**

**Fiscal year 2018 information technology (IT) funding request:** $1,549 million

**Development:** $138 million

**Operations and maintenance:** $1,411 million

**Official to whom the Chief Information Officer (CIO) reports:** Deputy Administrator

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 8

**Number of CIOs since 2012:** 4

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 2 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.9 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 2 years

**Tenure of current CIO:** 2.2 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 22: Extent to Which National Aeronautics and Space Administration Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | NE |
| Approve the selection of bureau CIOs | FE |
| Provide input into bureau CIO performance evaluations | FE |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Partially** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | PE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | PE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | PE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | NE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | PE |
| Develop and maintain information security policies, procedures, and control techniques | PE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of National Aeronautics and Space Administration policies. | GAO-18-93

## National Science Foundation

**National Science Foundation**

**Fiscal year 2018 information technology (IT) funding request:** $115 million

**Development:** $24 million

**Operations and maintenance:** $91 million

**Official to whom the Chief Information Officer (CIO) reports:** Director

**CIO appointment type:** Career

**Status of current CIO:** Acting

**Number of CIOs since 2004:** 4

**Number of CIOs since 2012:** 2

**Average tenure of CIOs (not including the current CIO) since 2004:** 4.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 5.6 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 5.6 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 5.6 years

**Tenure of current CIO:** 5 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 23: Extent to Which National Science Foundation Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Not at all** |
| Establish goals for improving agency operations through IT | NE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | PE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | NE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of National Science Foundation policies. | GAO-18-93

## Nuclear Regulatory Commission

**Nuclear Regulatory Commission**

**Fiscal year 2018 information technology (IT) funding request:** $159 million

**Development:** $6 million

**Operations and maintenance:** $153 million

**Official to whom the Chief Information Officer (CIO) reports:** Executive Director for Operations

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 5

**Number of CIOs since 2012:** 3

**Average tenure of CIOs (not including the current CIO) since 2004:** 3.3 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 4.7 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 2 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 4.7 years

**Tenure of current CIO:** 1.3 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 24: Extent to Which Nuclear Regulatory Commission Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | FE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Minimally** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | PE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Fully** |
| Have a significant role in IT planning, programming, and budgeting decisions | FE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Substantially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | PE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | FE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | PE |

Source: GAO analysis of Nuclear Regulatory Commission policies. | GAO-18-93

## Office of Personnel Management

**Office of Personnel Management**

**Fiscal year 2018 information technology (IT) funding request:** $141 million

**Development:** $30 million

**Operations and maintenance:** $111 million

**Official to whom the Chief Information Officer (CIO) reports:** Director

**CIO appointment type:** Career

**Status of current CIO**: Permanent

**Number of CIOs since 2004:** 9

**Number of CIOs since 2012:** 8

**Average tenure of CIOs (not including the current CIO) since 2004:** 2.7 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.1 months

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.1 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 1 year

**Tenure of current CIO:** 2 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 25: Extent to Which Office of Personnel Management Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Minimally** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | PE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | PE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | PE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Office of Personnel Management policies. | GAO-18-93

## Small Business Administration

**Small Business Administration**

**Fiscal year 2018 information technology (IT) funding request:** $98 million

**Development:** $21 million

**Operations and maintenance:** $77 million

**Official to whom the Chief Information Officer (CIO) reports:** Administrator

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 10

**Number of CIOs since 2012:** 6

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.4 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.3 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.1 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 1 .3 years

**Tenure of current CIO:** 1.2 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 26: Extent to Which Small Business Administration Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Partially** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | FE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | FE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | NE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | NE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | FE |

Source: GAO analysis of Small Business Administration policies. | GAO-18-93

## Social Security Administration

**Social Security Administration**

**Fiscal year 2018 information technology (IT) funding request:** $1,651 million

**Development:** $556 million

**Operations and maintenance:**

$1,096 million

**Official to whom the Chief Information Officer (CIO) reports:** Commissioner

**CIO appointment type:** Career

**Status of current CIO:** Appointment

**Number of CIOs since 2004:** 9

**Number of CIOs since 2012:** 6

**Average tenure of CIOs (not including the current CIO) since 2004:** 1.8 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 1.2 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.6 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 1.5 years

**Tenure of current CIO:** 6 months

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

**Table 27: Extent to Which Social Security Administration Policies Addressed the Role of Its Chief Information Officer (CIO)**

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Fully** |
| Report directly to the agency head or that official's deputy | FE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Minimally** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Substantially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | FE |
| **IT Investment Management** | **Partially** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | FE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | PE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | FE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | FE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | FE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Substantially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | FE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of Social Security Administration policies. | GAO-18-93

## U.S. Agency for International Development

**U.S. Agency for International Development**

**Fiscal year 2018 information technology (IT) funding request:** $141 million

**Development:** $26 million

**Operations and maintenance:** $115 million

**Official to whom the Chief Information Officer (CIO) reports:** Assistant Administrator of Bureau for Management

**CIO appointment type:** Career

**Status of current CIO:** Permanent

**Number of CIOs since 2004:** 7

**Number of CIOs since 2012:** 2

**Average tenure of CIOs (not including the current CIO) since 2004:** 2.1 years

**Average tenure of CIOs (not including the current CIO) since 2012:** 4.9 years

**Median tenure of CIOs (not including the current CIO) since 2004:** 1.3 years

**Median tenure of CIOs (not including the current CIO) since 2012:** 4.9 years

**Tenure of current CIO:** 3.8 years

Source: IT Dashboard and agency documentation, as of November 2017. | GAO-18-93

### Table 28: Extent to Which U.S. Agency for International Development Policies Addressed the Role of Its Chief Information Officer (CIO)

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| **Information Technology (IT) Leadership and Accountability** | **Substantially** |
| Report directly to the agency head or that official's deputy | NE |
| Assume responsibility and accountability for IT investments | FE |
| Approve the selection of bureau CIOs | N/A |
| Provide input into bureau CIO performance evaluations | N/A |
| Designate a senior agency information security officer | FE |
| **IT Strategic Planning** | **Minimally** |
| Establish goals for improving agency operations through IT | FE |
| Measure how well IT supports agency programs | NE |
| Prepare an annual report on the progress in achieving the goals | NE |
| Benchmark agency processes against private and public sector performance | NE |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | NE |
| **IT Workforce** | **Not at all** |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | NE |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | NE |
| Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies | NE |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | NE |
| **IT Budgeting** | **Partially** |
| Have a significant role in IT planning, programming, and budgeting decisions | PE |
| Ensure that the agency implements a process for selecting IT investments | FE |
| Review and approve the IT budget request | FE |
| Review and approve funding reprogramming requests | NE |
| **IT Investment Management** | **Minimally** |
| Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT | PE |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | NE |

| Responsibility to be addressed in agency policies | GAO analysis |
|---|---|
| Ensure that the agency implements a process for controlling and evaluating IT investments | FE |
| Evaluate IT investments according to risk (IT Dashboard CIO ratings) | NE |
| Review high-risk IT investments (TechStat sessions) | FE |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | NE |
| Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | FE |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | NE |
| Review and approve IT contracts, acquisition plans, or strategies | NE |
| Maintain an inventory of data centers | NE |
| Maintain a strategy to consolidate and optimize data centers | NE |
| **Information Security** | **Partially** |
| Develop and maintain an agency-wide information security program | FE |
| Develop and maintain information security policies, procedures, and control techniques | FE |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | NE |
| Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques | FE |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | NE |
| Report annually to the agency head on the effectiveness of the agency information security program | NE |

Source: GAO analysis of U.S. Agency for International Development policies. | GAO-18-93

# Appendix IV: Assessment of the Extent to Which Agencies' Policies Addressed the Role of Their CIOs, Arranged by Responsibility

The tables below provide additional detail on the 35 responsibilities in our Chief Information Officer (CIO) responsibility evaluation framework and our assessment of the extent to which the policies of the selected 24 agencies addressed each responsibility.

**Table 29: Extent to Which the 24 Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO) for the Area of Information Technology (IT) Leadership and Accountability**

Report to the agency head or that official's deputy.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 14 | Commerce, Defense, Education, Energy, Interior, Transportation, VA, EPA, GSA, NASA, NSF, OPM, SBA, and SSA |
| Partially | 0 | None |
| Not at all | 10 | Agriculture, HHS, DHS, HUD, Justice, Labor, State, Treasury, NRC, and USAID |

Assume responsibility and accountability for IT investments.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 22 | Agriculture, Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID |
| Partially | 0 | None |
| Not at all | 2 | EPA and NASA |

Approve the selection of bureau CIOs.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 10 | Agriculture, Commerce, Education, Energy, DHS, Interior, Justice, Labor, Transportation, and NASA |
| Partially | 0 | None |
| Not at all | 3 | HHS, HUD, and Treasury |
| N/A | 11 | This responsibility is not applicable to the following 10 agencies because they do not have bureau CIOs: State, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID. In addition, this responsibility does not apply to Defense because it was exempted from this responsibility under FITARA. |

Provide input into bureau CIO ratings.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 9 | Commerce, Education, Energy, HHS, Interior, Justice, Labor, Transportation, and NASA |
| Partially | 0 | None |
| Not at all | 5 | Agriculture, Defense, DHS, HUD, and Treasury |
| N/A | 10 | This responsibility is not applicable to the following 10 agencies because they do not have bureau CIOs: State, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID |

Designate a senior agency information security officer.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 22 | Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Justice, Labor, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |
| Partially | 0 | None |
| Not at all | 2 | Agriculture and State |

Source: GAO analysis of agency IT management policies. | GAO-18-93

Note: Agriculture (Department of Agriculture), Commerce (Department of Commerce), Defense (Department of Defense), Education (Department of Education), Energy (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), Interior (Department of the Interior), Justice (Department of Justice), Labor (Department of Labor), Transportation (Department of Transportation), Treasury (Department of the Treasury), State (Department of State), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), NASA (National Aeronautics and Space Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM (Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (U.S. Agency for International Development).

**Table 30: Extent to Which the 24 Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO) for the Area of Information Technology (IT) Strategic Planning**

Establish goals for improving agency operations through IT.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 15 | Commerce, Defense, Energy, HHS, HUD, Interior, Justice, Labor, EPA, NASA, NRC, OPM, SBA, SSA and USAID |
| Partially | 0 | None |
| Not at all | 9 | Agriculture, Education, DHS, State, Transportation, Treasury, VA, GSA, and NSF |

Measure performance of how well IT supports agency programs.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 12 | Commerce, Defense, Energy, HUD, Interior, Justice, Labor, GSA, NASA, NRC, OPM, and SBA |
| Partially | 0 | None |
| Not at all | 12 | Agriculture, Education, HHS, DHS, State, Transportation, Treasury, VA, EPA, NSF, SSA, and USAID |

Prepare an annual report on the progress in achieving the goals.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 4 | HUD, Justice, Labor, and NRC |
| Partially | 0 | None |
| Not at all | 20 | Agriculture, Commerce, Defense, Education, Energy, HHS, DHS, Interior, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, OPM, SBA, SSA, and USAID |

Benchmark agency processes against private and public sector performance.

| *Assessment* | | *Agencies and comments* |
|---|---|---|
| Fully | 0 | None |
| Partially | 1 | Although Justice established policies that call for the CIO to benchmark against public sector performance, the policies did not describe the CIO's role for benchmarking against private sector performance. |
| Not at all | 23 | Agriculture, Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |

Ensure that agency processes are analyzed and revised as appropriate before making significant investments.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 2 | Defense and SBA |
| Partially | 0 | None |
| Not at all | 22 | Agriculture, Commerce, Education, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SSA, and USAID |

Source: GAO analysis of agency IT management policies. | GAO-18-93

Note: Agriculture (Department of Agriculture), Commerce (Department of Commerce), Defense (Department of Defense), Education (Department of Education), Energy (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), Interior (Department of the Interior), Justice (Department of Justice), Labor (Department of Labor), Transportation (Department of Transportation), Treasury (Department of the Treasury), State (Department of State), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), NASA (National Aeronautics and Space Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM (Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (U.S. Agency for International Development).

**Table 31: Extent to Which the 24 Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO) for the Area of Information Technology (IT) Workforce**

Assess annually the requirements established for agency personnel regarding IT management knowledge and skills.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 4 | Agriculture, Labor, Transportation, and GSA |
| Partially | 6 | Although Defense, Interior, Justice, NASA, NRC, and OPM developed policies that call for their CIOs to establish requirements for agency personnel regarding IT management knowledge and skills, the policies did not require the CIOs to conduct these assessments on an annual basis. |
| Not at all | 14 | Commerce, Education, Energy, HHS, DHS, HUD, Interior, State, Treasury, VA, EPA, NSF, SBA, SSA, and USAID |

### Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 0 | None |
| Partially | 5 | Agriculture, Defense, Justice, Transportation, and NASA established policies that partially addressed the role of their CIOs for this responsibility. Although Defense, Justice, and NASA developed policies that call for their CIOs to assess the extent to which agency personnel meet IT management knowledge and skill requirements, the policies did not require their CIOs to conduct these assessments on an annual basis. With respect to Agriculture, although the agency established policies that call for skill gap assessments, these assessments were limited to evaluating skills for program and projects managers, and were not required to be performed annually. Regarding Transportation, although the agency established policies that call for annual skill gap assessments, these assessments were limited to evaluating skills for executives and management. |
| Not at all | 19 | Commerce, Education, Energy, HHS, DHS, HUD, Interior, Labor, State, Treasury, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID |

### Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 1 | Labor |
| Partially | 7 | Agriculture, Commerce, Defense, Justice, State, Transportation, and NASA established policies that partially addressed the role of their CIOs for this responsibility. Although Commerce, Defense, Justice, State, and NASA established policies that call for their CIOs to develop strategies for hiring and training to rectify any knowledge and skill deficiencies, the policies did not require the CIOs to develop these strategies on an annual basis. With respect to Agriculture and Transportation, although the agencies established policies that call for their CIOs to annually develop strategies to rectify knowledge and skill deficiencies, these strategies were limited to addressing deficiencies for executives and management. |
| Not at all | 16 | Education, Energy, HHS, DHS, HUD, Interior, Treasury, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID |

### Report annually to the head of the agency on progress made in improving IT personnel capabilities.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 1 | Labor |
| Partially | 1 | Although Agriculture established a policy that calls for its CIO to report annually on progress made in improving IT personnel capabilities, the policy did not call for the CIO to report to the head of the agency and the report was limited to progress made in improving skills for management. |
| Not at all | 22 | Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Justice, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |

Source: GAO analysis of agency IT management policies. | GAO-18-93

Note: Agriculture (Department of Agriculture), Commerce (Department of Commerce), Defense (Department of Defense), Education (Department of Education), Energy (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), Interior (Department of the Interior), Justice (Department of Justice), Labor (Department of Labor), Transportation (Department of Transportation), Treasury (Department of the Treasury), State (Department of State), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), NASA (National Aeronautics and Space Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM

(Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (U.S. Agency for International Development).

**Table 32: Extent to Which the 24 Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO) for the Area of Information Technology (IT) Budgeting**

Have a significant role in IT planning, programming, and budgeting decisions.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 3 | DHS, Justice, and NRC |
| Partially | 20 | Agriculture, Commerce, Education, Energy, HHS, HUD, Interior, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, OPM, SBA, SSA, and USAID developed policies that partially addressed the role of their CIOs for this responsibility. This responsibility is comprised of the following three elements: (1) define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages; (2) participate in the planning, programming, and budgeting stages for programs that include IT resources; and (3) approve the IT components of any plans through a process balancing IT investments with other uses of agency funding. The following describes the extent to which the 20 agencies addressed the these elements:<br>• **Define the level of detail with which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages.** Energy and Interior established policies that addressed the role of their CIOs for this element. Agriculture, Commerce, Education, HHS, HUD, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, OPM, SBA, SSA, and USAID did not establish policies that addressed the role of their CIOs for this element.<br>• **Participate in the planning, programming, and budgeting stages for programs that include IT resources.** All 20 agencies established policies that addressed the role of its CIO for this element.<br>• **Approve the IT components of any plans through a process balancing IT investments with other uses of agency funding.** Agriculture, Education, and SSA established policies that addressed the role of their CIOs for this element. Commerce, Energy, HHS, HUD, Interior, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, OPM, SBA, and USAID did not establish policies that addressed the role of their CIOs for this element. |
| Not at all | 0 | None |
| N/A | 1 | This responsibility does not apply to Defense because it was exempted from this responsibility under FITARA. |

Ensure that the agency implements a process for selecting IT investments.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 21 | Agriculture, Commerce, Defense, Education, HHS, DHS, HUD, Interior, Labor, State, Transportation, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |
| Partially | 2 | Energy and Justice established policies that partially addressed the role of their CIOs for this responsibility. With respect to Energy, although the agency established a policy that calls for the CIO to ensure that the agency implements a process for selecting most IT investments, Energy has exempted the Bonneville Power Administration's IT investments from this process. Regarding Justice, although the agency established policies that address the role of the CIO to ensure the agency implements a process for selecting critical or major IT investments, the policies did not address the role of the CIO for all other investments. |
| Not at all | 1 | Treasury |

Review and approve the IT budget request.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 16 | Agriculture, Commerce, Defense,[a] Education, Energy, DHS, HUD, Interior, Justice, EPA, GSA, NASA, NRC, OPM, SSA, and USAID |
| Partially | 5 | HHS, Labor, State, Treasury, and NSF established policies that partially addressed the role of their CIOs for this responsibility. Although Labor, State, Treasury, and NSF established policies that call for their CIOs to review the IT budget request, the policies did not require that the CIOs approve the IT budget requests. With respect to HHS, although the agency has established a policy that calls for the CIO to review and approve budgets for investments with planned costs over $20 million per year or $100 million over 5 years, the policy calls for bureau CIOs to review and approve all other investments. |
| Not at all | 3 | Transportation, VA, and SBA |

Review and approve funding reprogramming requests (i.e., shifting funds within an appropriation fund or account).

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 13 | Agriculture, Commerce, Education, DHS, Interior, Justice, Transportation, VA, GSA, NASA, NRC, OPM, and SSA |
| Partially | 0 | None |
| Not at all | 10 | Energy, HHS, HUD, Labor, State, Treasury, EPA, NSF, SBA, and USAID |
| N/A | 1 | This responsibility does not apply to Defense because it was exempted from this responsibility under FITARA. |

Source: GAO analysis of agency IT management policies. | GAO-18-93

Note: Agriculture (Department of Agriculture), Commerce (Department of Commerce), Defense (Department of Defense), Education (Department of Education), Energy (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), Interior (Department of the Interior), Justice (Department of Justice), Labor (Department of Labor), Transportation (Department of Transportation), Treasury (Department of the Treasury), State (Department of State), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), NASA (National Aeronautics and Space Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM (Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (U.S. Agency for International Development).

[a] This requirement applies differently to Defense under FITARA. Defense's CIO is required to review and provide recommendations on the IT budget request.

**Table 33: Extent to Which the 24 Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO) for the Area of Information Technology (IT) Investment Management**

Have a significant role in IT execution decisions and the management, governance, and oversight processes related to IT.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 0 | None |
| Partially | 23 | Agriculture, Commerce, Education, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID established policies that partially addressed the role of their CIOs for this responsibility. This responsibility is comprised of the following four elements: (1) establish and maintain a process to regularly engage with program managers to evaluate IT resources supporting each agency strategic objective; (2) define agency-wide policy for the level of detail of planned IT expenditure reporting; (3) define overall policies for capital planning, enterprise architecture, project management, and reporting for IT resources; and (4) participate on governance boards that include IT resources, including bureau investment review boards. The following describes the extent to which the 23 agencies addressed the these elements:<br>• **Establish and maintain a process to engage with program managers.** Education and OPM established policies that addressed the role of their CIOs for this element. Agriculture, Commerce, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, SBA, SSA, and USAID did not establish policies that addressed the role of their CIOs for this element.<br>• **Define agency-wide policy for the level of detail of planned IT expenditure reporting.** DHS, Interior, Justice, and Labor established policies that addressed the role of their CIOs for this element. Agriculture, Commerce, Education, Energy, HHS, HUD, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID did not establish policies that addressed the role of their CIOs for this element.<br>• **Define overall policies for capital planning, enterprise architecture, project management, and reporting for IT resources.** Agriculture, Energy, Interior, Justice, VA, and NRC established policies that addressed the role of their CIOs for this element. HUD did not establish policies that addressed this element. Commerce, Education, HHS, DHS, Labor, State, Transportation, Treasury, EPA, GSA, NASA, NSF, OPM, SBA, SSA, and USAID established policies that partially addressed this element.<br>o Commerce, Education, GSA, NASA, and USAID: The agencies established policies that addressed the role of their CIOs in defining overall policies for capital planning, enterprise architecture, and project management, but did not establish policies that addressed the role of their CIOs in defining overall policies for reporting for IT resources.<br>o HHS, Labor, State, EPA, NSF, SBA, and SSA: The agencies established policies that addressed the role of their CIOs in defining overall policies for capital planning and enterprise architecture, but did not establish policies that addressed the role of their CIOs in defining overall policies for project management and reporting for IT resources. |

| Assessment | | Agencies and comments |
|---|---|---|
| | | ○ OPM: The agency established policies that addressed the role of the CIO in defining overall policies for capital planning, but did not establish policies that addressed the role of the CIO in defining overall policies for enterprise architecture, project management, and reporting for IT resources.<br>○ DHS: The agency established policies that addressed the role of the CIO in defining overall policies for capital planning, enterprise architecture, and reporting for IT resources, but did not establish policies that addressed the role of the CIO in defining overall policies for project management.<br>○ Treasury: The agency established policies that addressed the role of the CIO in defining overall policies for capital planning, project management, and reporting for IT resources, but did not establish policies that addressed the role of the CIO in defining overall policies for enterprise architecture.<br>○ Transportation: The agency established policies that addressed the role of the CIO in defining overall policies for enterprise architecture, but did not establish policies that addressed the role of the CIO in defining overall policies for capital planning, project management, and reporting for IT resources.<br>• **Participate on governance boards that include IT resources, including bureau investment review boards.** Agriculture, Education, Treasury, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID established policies that addressed the role of their CIOs for this element. Commerce, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, and NASA addressed the role of their CIOs in some, but not all, IT governance boards. |
| Not at all | 0 | None |
| N/A | 1 | This responsibility does not apply to Defense because it was exempted from this responsibility under FITARA. |

## Improve the management of the agency's IT through portfolio review (PortfolioStat).

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 9 | Commerce, Defense, Education, Interior, Justice, Transportation, NRC, OPM, and SSA |
| Partially | 0 | None |
| Not at all | 15 | Agriculture, Energy, HHS, DHS, HUD, Labor, State, Treasury, VA, EPA, GSA, NASA, NSF, SBA, and USAID |

## Ensure that the agency implements a process for controlling and evaluating IT investments.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 21 | Agriculture, Commerce, Defense, Education, HHS, DHS, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, and USAID |
| Partially | 2 | Energy and SSA established policies that partially addressed the role of their CIOs for this responsibility. With respect to Energy, although the agency established policies that address the CIO's responsibility to ensure the agency implements a process for controlling and evaluating most IT investments, Energy has exempted the Bonneville Power Administration's IT investments from this process. Regarding SSA, although the agency established policies that address the role of the CIO to ensure it implements processes for controlling and evaluating major IT investments, the policies did not address the role of the CIO for non-major investments. |
| Not at all | 1 | HUD |

Evaluate IT investments according to risk (IT Dashboard CIO ratings).

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 12 | Agriculture, Defense, Education, Energy, Interior, Justice, Labor, Transportation, Treasury, EPA, NRC, and SSA |
| Partially | 1 | Although DHS established a policy for assessing risks of major IT investments, the CIO is not primarily responsible for the evaluations or associated risk ratings that are publicly reported for certain major IT investments. |
| Not at all | 11 | Commerce, HHS, HUD, State, VA, GSA, NASA, NSF, OPM, SBA, and USAID |

Review high-risk IT investments (TechStat sessions).

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 12 | Defense, Education, DHS, Justice, Labor, State, Transportation, Treasury, NRC, OPM, SSA, and USAID |
| Partially | 1 | Although HHS established a policy that addresses the role of the CIO in the process for identifying investments that should undergo a TechStat review, the policy did not define the role of the CIO in conducting the review. |
| Not at all | 11 | Agriculture, Commerce, Energy, HUD, Interior, VA, EPA, GSA, NASA, NSF, and SBA |

Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 5 | Commerce, Energy, DHS, Transportation, and SSA. |
| Partially | 10 | Education, Interior, Labor, State, Treasury, VA, GSA, NSF, NRC, and OPM established policies that partially addressed the role of their CIOs for this responsibility. With respect to Interior, Labor, State, Treasury, VA, GSA, NSF, NRC, and OPM, although the agencies established policies for incremental development certification, the policies did not describe the role of their CIOs in the certification processes. Regarding Education, although the agency's incremental development certification policy describes the CIO's role in the certification process, it did not include a description of how CIO certification would be documented. |
| Not at all | 9 | Agriculture, Defense, HHS, HUD, Justice, EPA, NASA, SBA, and USAID |

Advise the head of the agency on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 14 | Agriculture, Commerce, Defense, Education, HHS, Interior, Justice, Labor, GSA, NASA, OPM, SBA, SSA, and USAID |
| Partially | 3 | Although DHS, Transportation, and NRC established policies that addressed the role of their CIOs in advising leadership on whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIOs' evaluation, the agencies' policies direct the CIOs to provide this advice to senior leaders other than the agency head. |
| Not at all | 7 | Energy, HUD, State, Treasury, VA, EPA, and NSF |

Coordinate with the agency head and Chief Financial Officer to ensure that the financial systems are effectively established and implemented.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 4 | Commerce, Defense, Energy, and Justice |
| Partially | 1 | Although DHS established a policy that calls for the CIO and Chief Financial Officer to ensure that corrective action plans for financial IT systems are developed and implemented, this policy does not address the role of the CIO in coordinating with the Chief Financial Officer in other areas relating to financial systems, such as planning and budgeting decisions. |
| Not at all | 19 | Agriculture, Education, HHS, HUD, Interior, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |

Review and approve IT contracts, acquisition plans, or strategies.

| Assessment | | Comments |
|---|---|---|
| Fully | 8 | Commerce, HHS, EPA, GSA, NSF, NRC, SBA, and SSA |
| Partially | 9 | Agriculture, Education, DHS, HUD, Interior, Justice, Labor, Transportation, and OPM established policies that partially addressed the role of their CIOs for this responsibility. With respect to Agriculture, although the agency CIO or designee reviews and approves a subset of IT acquisition plans or strategies, the agency's processes do not currently allow for the approval of a particular acquisition strategy or plan. Regarding Education, although the agency has established a policy that states the Office of the CIO may review IT acquisition plans or strategies as one of several possible documents, reviewing acquisition plans and strategies is not required. Regarding DHS, although the agency has established a process for reviewing and approving IT contracts and agreements prior to award, these processes do not require contracts under certain thresholds to be approved by their CIOs. With regard to HUD and OPM, although the agencies have established processes whereby the CIOs have delegated approval authority for certain acquisitions to Office of the CIO officials, OMB has not yet approved these delegations. Regarding Interior and Justice, although the agencies have established policies that call for their CIOs to review and approve acquisition plans through governance boards, the agencies have yet to finalize charters for those boards. With respect to Transportation, although the agency has established a policy that calls for the CIO to approve acquisitions above a certain threshold by way of a governance board and has delegated authority for other acquisitions to bureau CIOs, OMB has not approved the delegations. Lastly, regarding Labor, although the agency has established a policy that calls for the CIO to review and approve IT acquisition plans associated with major investments, the policy does not require the CIO to do so for nonmajor investments. |
| Not at all | 6 | Energy, State, Treasury, VA, NASA, and USAID |
| N/A | 1 | This responsibility does not apply to Defense because it was exempted from this responsibility under FITARA. |

Maintain an inventory of data centers.

| Assessment | | Comments |
|---|---|---|
| Fully | 3 | Defense, State, and NRC |
| Partially | 0 | None |
| Not at all | 19 | Agriculture, Commerce, Energy, HHS, DHS, Interior, Justice, Labor, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, OPM, SBA, SSA, and USAID |
| N/A | 2 | This responsibility does not apply to Education and HUD because these agencies do not have any agency-owned data centers. |

Maintain a strategy to consolidate and optimize data centers.

| Assessment | | Comments |
|---|---|---|
| Fully | 2 | Defense and State |
| Partially | 0 | None |
| Not at all | 20 | Agriculture, Commerce, Energy, HHS, DHS, Interior, Justice, Labor, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |
| N/A | 2 | This responsibility does not apply to Education and HUD because these agencies do not have any agency-owned data centers. |

Source: GAO analysis of agency IT management policies. | GAO-18-93

Note: Agriculture (Department of Agriculture), Commerce (Department of Commerce), Defense (Department of Defense), Education (Department of Education), Energy (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), Interior (Department of the Interior), Justice (Department of Justice), Labor (Department of Labor), Transportation (Department of Transportation), Treasury (Department of the Treasury), State (Department of State), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), NASA (National Aeronautics and Space Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM (Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (U.S. Agency for International Development).

**Table 34: Extent to Which the 24 Agencies' Policies Defined the Role of Their Chief Information Officers (CIO) in the Area of Information Security**

Develop and maintain an agency-wide information security program.

| *Assessment* | | *Agencies and comments* |
|---|---|---|
| Fully | 23 | Agriculture, Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID |
| Partially | 1 | Although NASA established a policy that calls for the CIO to develop and maintain a NASA-wide information program, the policy also assigned the NASA Assistant Administrator for the Office of Protective Services the responsibility to establish a program, in collaboration with the CIO, for the oversight and protection of classified national security information. |
| Not at all | 0 | None |

Develop and maintain information security policies, procedures, and control techniques.

| *Assessment* | | *Agencies and comments* |
|---|---|---|
| Fully | 20 | Agriculture, Commerce, Defense, Education, HHS, DHS, Interior, Justice, Labor, State, Transportation, VA, EPA, GSA, NSF, NRC, OPM, SBA, SSA, and USAID |
| Partially | 3 | Energy, Treasury, and NASA established policies that partially addressed the role of their CIOs for this responsibility. Although Energy, Treasury, and NASA established policies that call for their CIOs to develop and maintain security policies and procedures, the policies did not address the role of their CIOs with respect to control techniques. |
| Not at all | 1 | HUD |

Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 6 | Defense, Interior, Justice, VA, EPA, and SSA |
| Partially | 0 | None |
| Not at all | 18 | Agriculture, Commerce, Education, Energy, HHS, DHS, HUD, Labor, State, Transportation, Treasury, GSA, NASA, NSF, NRC, OPM, SBA, and USAID |

Ensure that agency personnel, including those with significant responsibility for information security, are trained to effectively carry out information security policies, procedures, and control techniques.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 24 | Agriculture, Commerce, Defense, Education, Energy, HHS, DHS, HUD, Interior, Justice, Labor, State, Transportation, Treasury, VA, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |
| Partially | 0 | None |
| Not at all | 0 | None |

Ensure that all personnel are held accountable for complying with the agency-wide information security program.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 3 | Defense, Justice, and VA |
| Partially | 0 | None |
| Not at all | 21 | Agriculture, Commerce, Education, Energy, HHS, DHS, HUD, Interior, Labor, State, Transportation, Treasury, EPA, GSA, NASA, NSF, NRC, OPM, SBA, SSA, and USAID |

Report annually to the agency head on the effectiveness of the agency information security program.

| Assessment | | Agencies and comments |
|---|---|---|
| Fully | 12 | Agriculture, Energy, HHS, DHS, Justice, Transportation, VA, EPA, GSA, NSF, OPM, and SBA |
| Partially | 4 | Although Commerce, Defense, Labor, and NRC have established policies that call for their CIOs to report annually on the effectiveness of their information security programs, the policies did not address the responsibility to provide the reports to the heads of these agencies. |
| Not at all | 8 | Education, HUD, Interior, State, Treasury, NASA, SSA, and USAID |

Source: GAO analysis of agency IT management policies. | GAO-18-93

Note: Agriculture (Department of Agriculture), Commerce (Department of Commerce), Defense (Department of Defense), Education (Department of Education), Energy (Department of Energy), HHS (Department of Health and Human Services), DHS (Department of Homeland Security), HUD (Department of Housing and Urban Development), Interior (Department of the Interior), Justice (Department of Justice), Labor (Department of Labor), Transportation (Department of Transportation), Treasury (Department of the Treasury), State (Department of State), VA (Department of Veterans Affairs), EPA (Environmental Protection Agency), NASA (National Aeronautics and Space Administration), NSF (National Science Foundation), NRC (Nuclear Regulatory Commission), OPM (Office of Personnel Management), SBA (Small Business Administration), SSA (Social Security Administration), USAID (U.S. Agency for International Development).

# Appendix V: Responses to Survey on CIO Responsibilities

The questions we asked in our survey of Chief Information Officers (CIO) are shown below. Our survey was comprised of closed- and open-ended questions. This appendix includes aggregate results of responses to the closed-ended questions. For a more detailed discussion of our survey methodology, see appendix I.

## SECTION 1: IT Leadership and Accountability

1. **How effective, if at all, have you been in carrying out each of the following responsibilities related to IT Leadership and Accountability?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable |
|---|---|---|---|---|---|
| Ensure effective implementation of IT management responsibilities | 0 | 1 | 14 | 9 | 0 |
| Ensure effective implementation of information security responsibilities | 0 | 0 | 9 | 15 | 0 |
| Assume responsibility and accountability for IT investments | 0 | 5 | 13[a] | 7[a] | 0 |
| Provide input into bureau CIO performance evaluations (In this survey, bureau means the principal subordinate organizational units of an agency (e.g., components, services, operating divisions.)) | 1 | 2 | 6 | 7 | 8 |
| Provide advice and assistance to the agency head | 0 | 0 | 6 | 17 | 1 |

[a] One CIO responded as being both somewhat effective and very effective. This response is reflected in the number of CIOs for both categories.

2. **Have you been able to effectively carry out each of the following responsibilities?** Please check one box in each row.

| Responsibility | Yes | No | Not applicable |
|---|---|---|---|
| Report directly to the agency head | 15 | 9 | 0 |
| Approve the selection of bureau CIOs | 13 | 3 | 8 |
| Designate a chief information security officer | 24 | 0 | 0 |

3. **Overall, how effective, if at all, have you been in carrying out the above responsibilities related to IT Leadership and Accountability?** Please check one box.

| Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|
| 0 | 2 | 10 | 11 | 0 | 1 |

4. **Do you have sufficient access to the agency head to advise him or her on the following responsibilities?** Please check one box in each row.

| Responsibility | Yes | No | Not applicable | No basis to judge |
|---|---|---|---|---|
| IT management (i.e., IT strategic planning; IT workforce; IT planning, programming, and budgeting; and IT investment management) | 21 | 3 | 0 | 0 |
| Information security | 20 | 4 | 0 | 0 |

5. **Does the agency head provide you with sufficient authority to make decisions on IT?** Please check one box.

| Yes | No | Not applicable | No basis to judge |
|---|---|---|---|
| 22 | 2 | 0 | 0 |

6. **How much, if at all, is the agency head an advocate of the decisions you make on IT?** Please check one box.

| Not at all | Slightly | Somewhat | Very much | Not applicable | No basis to judge |
|---|---|---|---|---|---|
| 0 | 0 | 4 | 18 | 0 | 2 |

## SECTION 2: IT Strategic Planning

7. **How effective, if at all, have you been in carrying out each of the following responsibilities related to IT Strategic Planning?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable |
|---|---|---|---|---|---|
| Establish goals for improving agency operations through IT | 0 | 1 | 11 | 12 | 0 |
| Measure how well IT supports agency programs | 0 | 9 | 10 | 5 | 0 |
| Prepare an annual report on progress in achieving operational goals | 2 | 4 | 9 | 6 | 3 |
| Benchmark agency processes against private and public sector performance | 2 | 10 | 7 | 1 | 4 |
| Ensure that agency processes are analyzed and revised as appropriate before making significant IT investments | 3 | 6 | 10 | 5 | 0 |

8. **Overall, how effective, if at all, have you been in carrying out the above responsibilities related to IT Strategic Planning?** Please check one box.

| Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable |
|---|---|---|---|---|
| 0 | 6 | 12 | 5 | 1 |

## SECTION 3: IT Workforce

9. **How effective, if at all, have you been in carrying out each of the following responsibilities?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|---|
| Select office of the CIO employees according to required qualifications | 0 | 2 | 4 | 17 | 1 | 0 |
| Identify, recruit, and hire potential applicants to lead major IT programs (In this survey, a major IT program or investment means, among other things, an IT investment that requires special management attention because of its importance to the mission or function of the government.) | 3 | 2 | 13 | 6 | 0 | 0 |
| Provide annual performance reviews for officials leading major IT programs | 7[a] | 2 | 2 | 12[a] | 2 | 0 |
| Annually assess the requirements established for agency personnel regarding IT management and information security knowledge and skills | 2 | 6 | 7 | 9 | 0 | 0 |
| Annually assess the extent to which agency personnel meet IT management and information security knowledge and skill requirements | 2 | 7 | 8 | 7 | 0 | 0 |
| Annually develop strategies to rectify any knowledge and skill deficiencies (e.g., hiring and training) | 3 | 6 | 9 | 5 | 1 | 0 |
| Report annually to the head of the agency on progress made in improving IT personnel capabilities | 3 | 4 | 7 | 5 | 4 | 1 |

[a] One CIO responded as being both not at all effective and very effective. This response is reflected in the number of CIOs for both categories.

10. **Overall, how effective, if at all, have you been in carrying out the above responsibilities related to IT Workforce?** Please check one box.

| Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|
| 2 | 6 | 11 | 4 | 0 | 1 |

## SECTION 4: IT Planning, Programming, and Budgeting

11. **How effective, if at all, have you been in carrying out each of the following responsibilities related to IT Planning, Programming, and Budgeting?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable |
|---|---|---|---|---|---|
| Have a significant role in IT planning, programming, and budgeting decisions | 0 | 2 | 9 | 13 | 0 |
| Ensure that the agency implements a process for selecting IT investments | 0 | 1 | 8[a] | 16[a] | 0 |
| Ensure that the process for selecting IT investments is integrated with budget and financial decisions | 0 | 3 | 7 | 14 | 0 |
| Ensure that the process for selecting IT investments is integrated with program management decisions | 0 | 2 | 11 | 11 | 0 |
| Review and approve the IT budget request | 0 | 4 | 6[a] | 15[a] | 0 |
| Review and approve funding reprogramming requests (reprogramming requests refer to any movement of funds for IT resources that requires Congressional notification) | 2 | 1 | 6 | 9 | 6 |

[a] One CIO responded as being both somewhat effective and very effective. This response is reflected in the number of CIOs for both categories.

12. **Overall, how effective, if at all, have you been in carrying out the above responsibilities related to IT Planning, Programming, and Budgeting?** Please check one box.

| Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|
| 0 | 2 | 8 | 13 | 0 | 1 |

13. **How clearly, if at all, are IT resources and non-IT resources separated in a way that enables you to provide effective management and oversight specifically for IT resources?** Please check one box.

| Not at all clearly | Slightly clearly | Somewhat clearly | Very clearly | Not applicable | No basis to judge |
|---|---|---|---|---|---|
| 2 | 5 | 10 | 6 | 0 | 1 |

14. **Approximately what percentage of the agency's major IT investments did you approve for inclusion in the President's Fiscal Year 2017 budget?** Please check one box.

| 0% | > 0% but < 25% | 25% to < 50% | 50% to < 75% | 75% to < 100% | 100% | Not applicable | Don't know | No basis to judge |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 3 | 7 | 12 | 0 | 0 | 1 |

15. **For approximately what percentage of the agency's IT portfolio do you have the ability (whether individually or through a larger governance board) to prevent a planned IT investment from being included in your agency's budget?** Please check one box.

| 0% | > 0% but < 25% | 25% to < 50% | 50% to < 75% | 75% to < 100% | 100% | Not applicable | No basis to judge |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 3 | 7 | 8 | | 3 |

## SECTION 5: IT Investment Management

16. **How effective, if at all, have you been in carrying out each of the following responsibilities related to IT Investment Management?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|---|
| Have a significant role in IT execution decisions | 0 | 5 | 10 | 8 | 1 | 0 |
| Have a significant role in the management, governance, and oversight processes related to IT | 0 | 1 | 7 | 16 | 0 | 0 |
| Participate on governance boards that include IT resources, including bureau investment review boards | 0 | 1 | 9 | 14 | 0 | 0 |
| Improve the management of the agency IT portfolio through PortfolioStat | 0 | 6 | 10 | 8 | 0 | 0 |
| Ensure that the agency implements a process for controlling and evaluating IT investments | 0 | 3 | 4 | 17 | 0 | 0 |
| Ensure that this process for controlling and evaluating IT investments is integrated with budget and financial decisions | 0 | 5 | 9 | 10 | 0 | 0 |
| Ensure that the process for controlling and evaluating IT investments is integrated with program management decisions | 0 | 6 | 12 | 6 | 0 | 0 |
| Evaluate IT investments according to risk | 1 | 5 | 8 | 10 | 0 | 0 |
| Report the IT investment evaluations to the IT Dashboard | 1 | 4 | 4 | 15 | 0 | 0 |
| Review high-risk IT investments using TechStat sessions | 2 | 3 | 3 | 13 | 3 | 0 |
| Certify that investments are adequately implementing incremental development consistent with the Office of Management and Budget capital planning guidance | 1 | 3 | 11 | 9 | 0 | 0 |
| Provide the means for senior management to obtain information on the progress of all investments with an IT component (including measures of cost, timeliness, and quality) | 2 | 3 | 8 | 10 | 0 | 1 |
| Advise head of the agency whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component based on the CIO's evaluation | 1 | 1 | 5 | 14 | 3 | 0 |
| Have a lead role in managing the agency's commodity IT | 0 | 3 | 10 | 11 | 0 | 0 |
| Ensure that financial systems are effectively implemented | 1 | 8 | 7 | 7 | 1 | 0 |

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|---|
| Review and approve IT contracts | 2 | 6 | 8 | 8 | 0 | 0 |
| Maintain an inventory of data centers | 0 | 1 | 8 | 15 | 0 | 0 |
| Maintain a strategy to consolidate and optimize data centers | 0 | 2 | 5 | 17 | 0 | 0 |

17. **Overall, how effective, if at all, have you been in carrying out the above responsibilities related to IT Investment Management?** Please check one box.

| Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|
| 0 | 2 | 12 | 9 | 0 | 1 |

18. **For approximately what percentage of the agency's IT budget do you have the ability (whether individually or through a larger governance board) to cancel an IT investment that was previously approved?** Please check one box.

| 0% | > 0% but < 25% | 25% to < 50% | 50% to < 75% | 75% to < 100% | 100% | Not applicable | No basis to judge |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 1 | 1 | 8 | 8 | 0 | 3 |

## SECTION 6: Information Security

19. **How effective, if at all, have you been in carrying out each of the following responsibilities?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable |
|---|---|---|---|---|---|
| Develop and maintain an agency-wide information security program | 0 | 1 | 6 | 17 | 0 |
| Establish and implement information security policies, procedures, and control techniques | 0 | 1 | 7 | 16 | 0 |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | 0 | 2 | 8 | 13 | 1 |
| Ensure that agency personnel are trained to effectively carry out information security policies, procedures, and control techniques | 0 | 2 | 13 | 9 | 0 |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | 0 | 3 | 11 | 10 | 0 |
| Report annually to the agency head on the effectiveness of the agency information security program | 0 | 0 | 4 | 19 | 1 |

20. **How effective, if at all, have you been in ensuring the development and implementation of the following Federal Information Security Management Act (FISMA) elements of an information security program and risk management framework?** Please check one box in each row.

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No basis to judge | No response |
|---|---|---|---|---|---|---|---|
| A process for conducting information security risk assessments | 0 | 2 | 8 | 14 | 0 | 0 | 0 |
| Information security policies and procedures | 0 | 2 | 8 | 13 | 0 | 0 | 1 |
| Plans for providing adequate information security | 0 | 1 | 10 | 13 | 0 | 0 | 0 |
| A process for conducting information security awareness training | 0 | 0 | 8 | 16 | 0 | 0 | 0 |
| A process for testing and evaluating the effectiveness of information security policies | 0 | 3 | 10[a] | 12[a] | 0 | 0 | 0 |
| A process for planning and implementing remedial actions to address information security deficiencies | 0 | 3 | 9 | 12 | 0 | 0 | 0 |
| Procedures for detecting, reporting, and responding to security incidents | 0 | 1 | 6 | 17 | 0 | 0 | 0 |

| Responsibility | Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No basis to judge | No response |
|---|---|---|---|---|---|---|---|
| Plans and procedures to ensure continuity of operations for information systems | 1 | 1 | 11 | 11 | 0 | 0 | 0 |

[a] One CIO responded as being both somewhat effective and very effective. This response is reflected in the number of CIOs for both categories.

21. **<u>Overall</u>, how effective, if at all, have you been in carrying out the above responsibilities related to Information Security?** Please check one box.

| Not at all effective | Slightly effective | Somewhat effective | Very effective | Not applicable | No response |
|---|---|---|---|---|---|
| 0 | 1 | 9 | 13 | 0 | 1 |

## SECTION 7: Ranking CIO Responsibility Areas

22. **Please rank how challenging each CIO responsibility area has been to carry out in fiscal year 2016 by selecting a responsibility from the right column for each rank level below Please complete all six ranks below**. Please check only one box for each rank.

| Responsibility | Most challenging responsibility to carry out | Second-most challenging responsibility to carry out | Third-most challenging responsibility to carry out | Fourth-most challenging responsibility to carry out | Fifth-most challenging responsibility to carry out | Least challenging responsibility to carry out |
|---|---|---|---|---|---|---|
| Leadership and Accountability | 5 | 3 | 2 | 1 | 6 | 7 |
| IT Strategic Planning | 0 | 1 | 3 | 5 | 5 | 10 |
| IT Workforce | 7 | 5 | 5 | 4 | 1 | 1 |
| IT Planning, Programming, and Budgeting | 4 | 6 | 7 | 3 | 4 | 0 |
| IT Investment Management | 2 | 5 | 3 | 7 | 6 | 2 |
| Information Security | 6 | 4 | 4 | 4 | 2 | 4 |

23. **Approximately what percentage of time over fiscal year 2016 have you spent on each responsibility below?** Please enter a number in the space provided. **These percentages do not need to total 100 percent.**

| Responsibility | Minimum percentage | Maximum percentage | Median percentage | Mean percentage |
|---|---|---|---|---|
| Leadership and Accountability | 10 | 60 | 25 | 26.7 |
| IT Strategic Planning | 5 | 60 | 10 | 15.2 |
| IT Workforce | 0 | 40 | 15 | 13.9 |
| IT Planning, Programming, and Budgeting | 5 | 50 | 15 | 18.9 |
| IT Investment Management | 0 | 30 | 10 | 14.1 |
| Information Security | 5 | 75 | 25 | 29.9 |

Note: One CIO did not respond to this question.

## SECTION 8: Factors That Enabled and Challenged Your Ability to Effectively Carry Out Your Responsibilities

24. **How much has each of the following factors enabled or challenged your ability to effectively carry out your IT management and information security responsibilities?** Please check one box in each row.

| Responsibility | Major enabling factor | Minor enabling factor | Neither enabling nor challenging | Minor challenging factor | Major challenging factor | Not applicable | No response |
|---|---|---|---|---|---|---|---|
| National Institute of Standards and Technology (NIST) guidance | 14 | 3 | 4 | 3 | 0 | 0 | 0 |
| Office of Management and Budget guidance | 13[a] | 3[b] | 1 | 4[b] | 4[a] | 1 | 0 |
| Agency directives | 8 | 6 | 6 | 2 | 0 | 1 | 1 |
| Agency procedures | 7 | 8 | 3 | 4 | 1 | 1 | 0 |
| Policy writing authority | 9 | 7 | 6 | 2 | 0 | 0 | 0 |
| Legal authority | 12 | 2[b] | 6 | 4[b] | 0 | 1 | 0 |
| CIO position in agency hierarchy | 13 | 4 | 2 | 2 | 3 | 0 | 0 |
| Delegation of responsibilities | 10 | 5 | 4 | 3 | 1 | 1 | 0 |
| Oversight of indirect reports | 5 | 3[c] | 7 | 5 | 5[c] | 0 | 0 |
| Oversight of IT contractors | 4 | 2 | 9 | 6 | 1 | 2 | 0 |
| Availability of personnel/staff resources | 3 | 1 | 1 | 7 | 12 | 0 | 0 |
| Level of IT staff expertise | 4 | 3 | 1 | 9 | 7 | 0 | 0 |
| Processes for hiring, recruiting, and retaining IT personnel | 1 | 0 | 3 | 3 | 17 | 0 | 0 |

| Responsibility | Major enabling factor | Minor enabling factor | Neither enabling nor challenging | Minor challenging factor | Major challenging factor | Not applicable | No response |
|---|---|---|---|---|---|---|---|
| Coordination with the Chief Acquisition Officer or his/her office | 12[a] | 6 | 1 | 2 | 4[a] | 0 | 0 |
| Coordination with the Chief Financial Officer or his/her office | 11 | 7 | 3 | 2 | 1 | 0 | 0 |
| Coordination with the Chief Human Capital Officer or his/her office | 8 | 7 | 1 | 5 | 2 | 1 | 0 |
| Coordination elsewhere in the agency | 5 | 5 | 5 | 6 | 3 | 0 | 0 |
| Coordination with bureau CIOs | 9 | 0 | 4 | 2 | 2 | 7 | 0 |
| Ability to coordinate with external agencies | 4 | 7 | 12 | 1 | 0 | 0 | 0 |
| Information provided from internal organizations | 6 | 5 | 5 | 6 | 2 | 0 | 0 |
| Information provided from contractors/ contractor-owned systems | 0 | 5 | 11 | 3 | 4 | 1 | 0 |
| Institutional knowledge at the agency | 8 | 9 | 4 | 2 | 1 | 0 | 0 |
| Prioritization of agency operations and IT needs | 7 | 5 | 2 | 6 | 4 | 0 | 0 |
| Organizational culture at agency | 2 | 5 | 1 | 9 | 7 | 0 | 0 |
| Financial resources | 3[d] | 3[e] | 3[d, e] | 3 | 14 | 0 | 0 |

[a] One CIO responded that this factor was both a major enabling factor and a major challenging factor. This response is reflected in the number of CIOs for both categories.

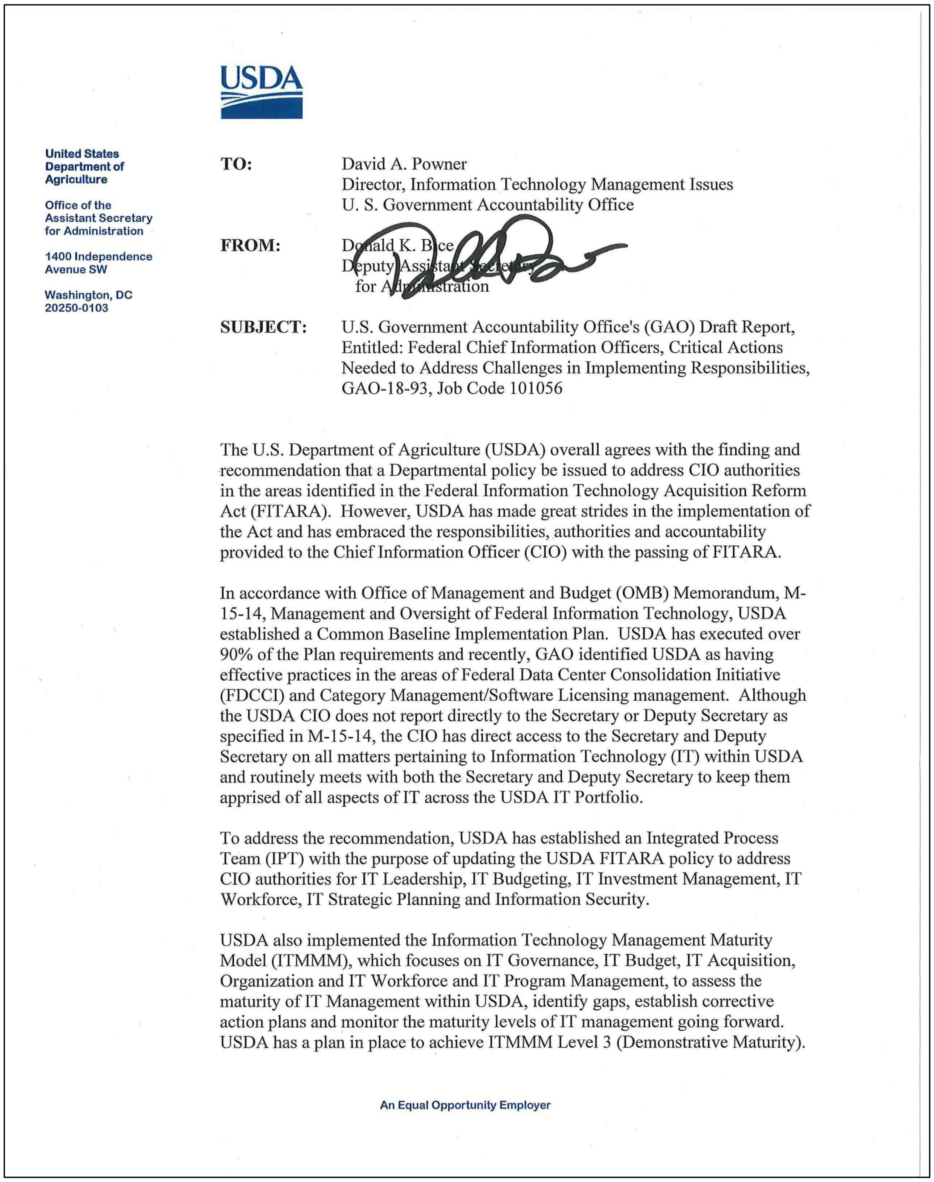
[b] One CIO responded that this factor was both a minor enabling factor and a minor challenging factor. This response is reflected in the number of CIOs for both categories.

[c] One CIO responded that this factor was both a minor enabling factor and a major challenging factor. This response is reflected in the number of CIOs for both categories.

[d] One CIO responded that this factor was both a major enabling factor and was also neither enabling nor challenging. This response is reflected in the number of CIOs for both categories.

[e] One CIO responded that this factor was both a minor enabling factor and was also neither enabling nor challenging. This response is reflected in the number of CIOs for both categories.

# Appendix VI: Comments from the Department of Agriculture



USDA

United States Department of Agriculture

Office of the Assistant Secretary for Administration

1400 Independence Avenue SW

Washington, DC 20250-0103

| | |
|---|---|
| **TO:** | David A. Powner<br>Director, Information Technology Management Issues<br>U. S. Government Accountability Office |
| **FROM:** | Donald K. Bice<br>Deputy Assistant Secretary<br>for Administration |
| **SUBJECT:** | U.S. Government Accountability Office's (GAO) Draft Report, Entitled: Federal Chief Information Officers, Critical Actions Needed to Address Challenges in Implementing Responsibilities, GAO-18-93, Job Code 101056 |

The U.S. Department of Agriculture (USDA) overall agrees with the finding and recommendation that a Departmental policy be issued to address CIO authorities in the areas identified in the Federal Information Technology Acquisition Reform Act (FITARA). However, USDA has made great strides in the implementation of the Act and has embraced the responsibilities, authorities and accountability provided to the Chief Information Officer (CIO) with the passing of FITARA.

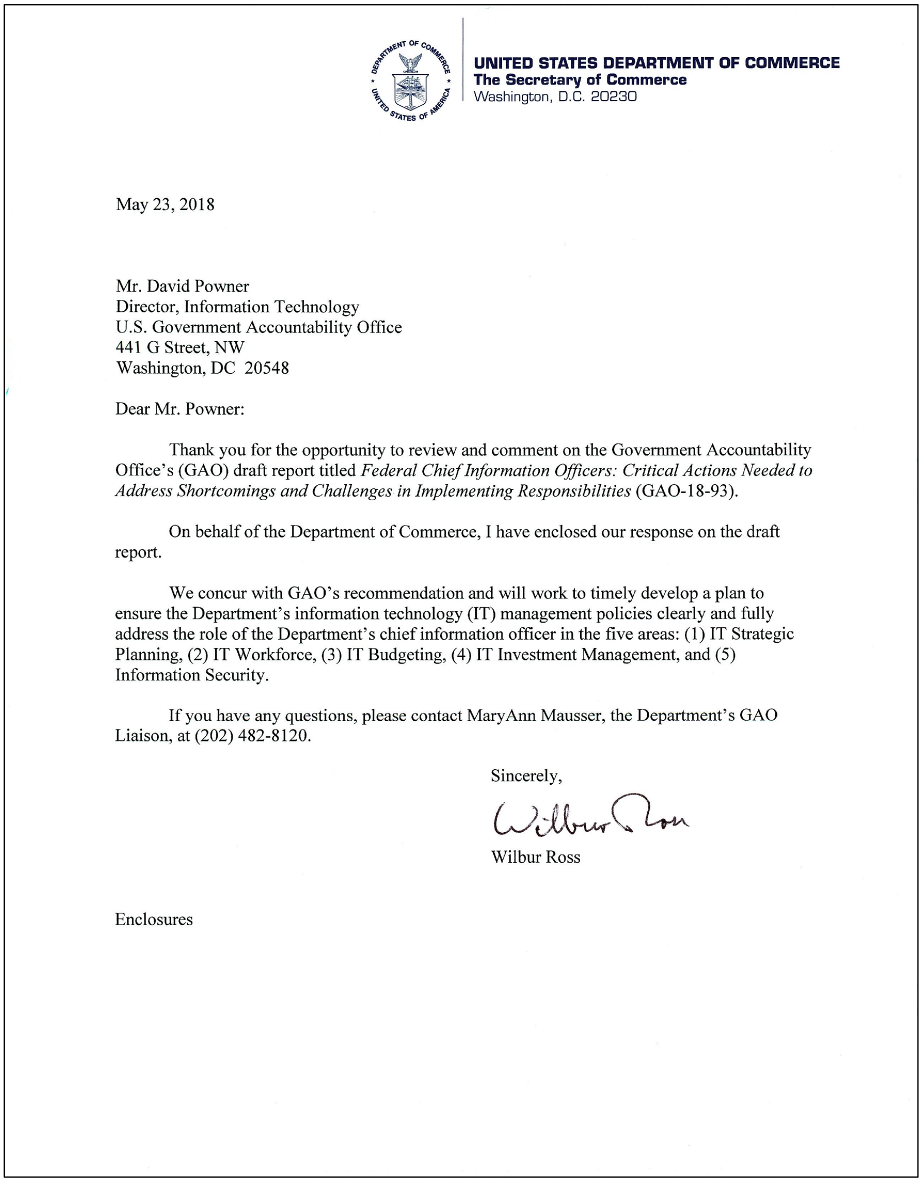
In accordance with Office of Management and Budget (OMB) Memorandum, M-15-14, Management and Oversight of Federal Information Technology, USDA established a Common Baseline Implementation Plan. USDA has executed over 90% of the Plan requirements and recently, GAO identified USDA as having effective practices in the areas of Federal Data Center Consolidation Initiative (FDCCI) and Category Management/Software Licensing management. Although the USDA CIO does not report directly to the Secretary or Deputy Secretary as specified in M-15-14, the CIO has direct access to the Secretary and Deputy Secretary on all matters pertaining to Information Technology (IT) within USDA and routinely meets with both the Secretary and Deputy Secretary to keep them apprised of all aspects of IT across the USDA IT Portfolio.

To address the recommendation, USDA has established an Integrated Process Team (IPT) with the purpose of updating the USDA FITARA policy to address CIO authorities for IT Leadership, IT Budgeting, IT Investment Management, IT Workforce, IT Strategic Planning and Information Security.

USDA also implemented the Information Technology Management Maturity Model (ITMMM), which focuses on IT Governance, IT Budget, IT Acquisition, Organization and IT Workforce and IT Program Management, to assess the maturity of IT Management within USDA, identify gaps, establish corrective action plans and monitor the maturity levels of IT management going forward. USDA has a plan in place to achieve ITMMM Level 3 (Demonstrative Maturity).

An Equal Opportunity Employer

# Appendix VII: Comments from the Department of Commerce



**UNITED STATES DEPARTMENT OF COMMERCE**
**The Secretary of Commerce**
Washington, D.C. 20230

May 23, 2018

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

Dear Mr. Powner:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* (GAO-18-93).

On behalf of the Department of Commerce, I have enclosed our response on the draft report.

We concur with GAO's recommendation and will work to timely develop a plan to ensure the Department's information technology (IT) management policies clearly and fully address the role of the Department's chief information officer in the five areas: (1) IT Strategic Planning, (2) IT Workforce, (3) IT Budgeting, (4) IT Investment Management, and (5) Information Security.

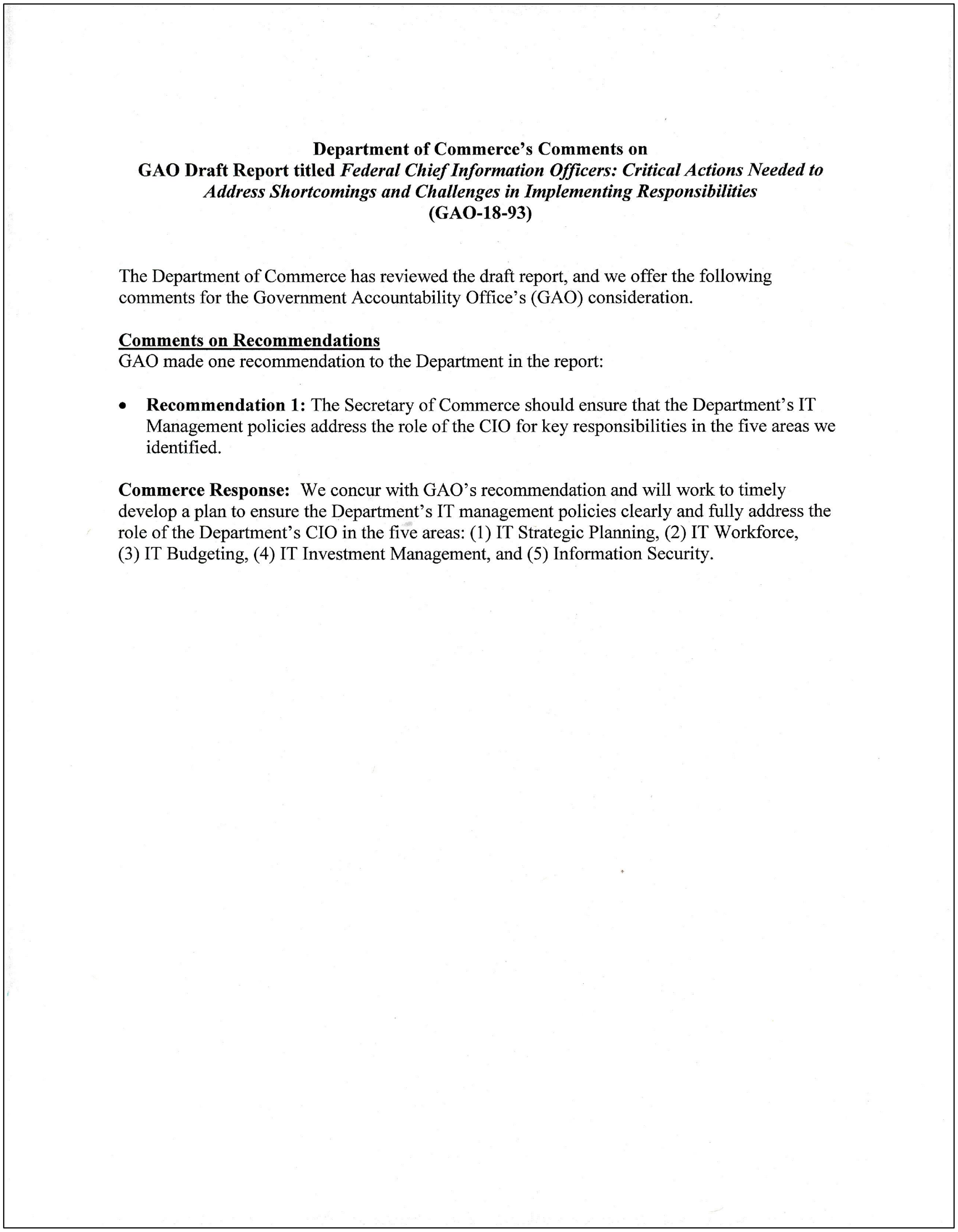
If you have any questions, please contact MaryAnn Mausser, the Department's GAO Liaison, at (202) 482-8120.

Sincerely,

Wilbur Ross

Wilbur Ross

Enclosures



**Department of Commerce's Comments on**
**GAO Draft Report titled *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities***
**(GAO-18-93)**

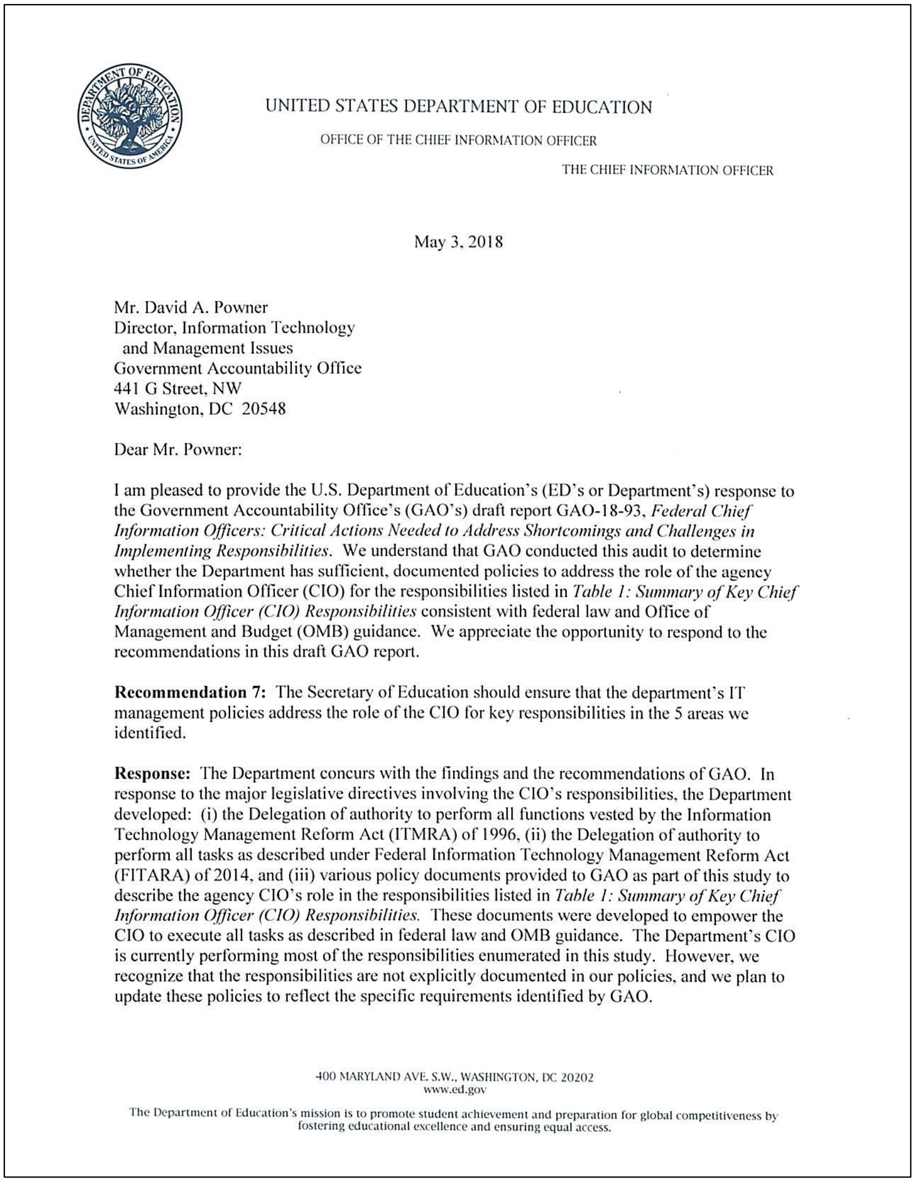
The Department of Commerce has reviewed the draft report, and we offer the following comments for the Government Accountability Office's (GAO) consideration.

**Comments on Recommendations**
GAO made one recommendation to the Department in the report:

- **Recommendation 1:** The Secretary of Commerce should ensure that the Department's IT Management policies address the role of the CIO for key responsibilities in the five areas we identified.

**Commerce Response:** We concur with GAO's recommendation and will work to timely develop a plan to ensure the Department's IT management policies clearly and fully address the role of the Department's CIO in the five areas: (1) IT Strategic Planning, (2) IT Workforce, (3) IT Budgeting, (4) IT Investment Management, and (5) Information Security.

# Appendix VIII: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

May 3, 2018

Mr. David A. Powner
Director, Information Technology
and Management Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

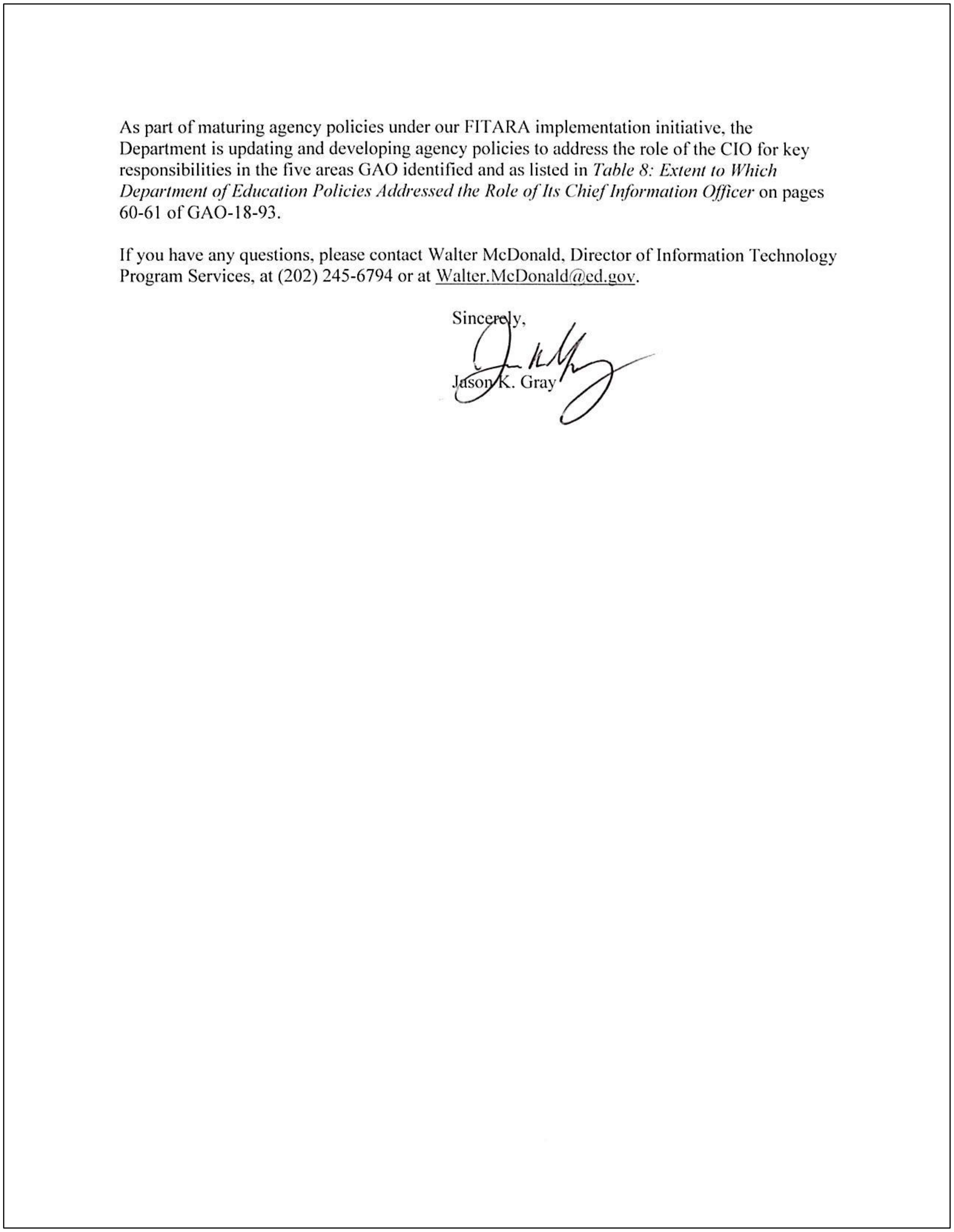
I am pleased to provide the U.S. Department of Education's (ED's or Department's) response to the Government Accountability Office's (GAO's) draft report GAO-18-93, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*. We understand that GAO conducted this audit to determine whether the Department has sufficient, documented policies to address the role of the agency Chief Information Officer (CIO) for the responsibilities listed in *Table 1: Summary of Key Chief Information Officer (CIO) Responsibilities* consistent with federal law and Office of Management and Budget (OMB) guidance. We appreciate the opportunity to respond to the recommendations in this draft GAO report.

**Recommendation 7:** The Secretary of Education should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified.

**Response:** The Department concurs with the findings and the recommendations of GAO. In response to the major legislative directives involving the CIO's responsibilities, the Department developed: (i) the Delegation of authority to perform all functions vested by the Information Technology Management Reform Act (ITMRA) of 1996, (ii) the Delegation of authority to perform all tasks as described under Federal Information Technology Management Reform Act (FITARA) of 2014, and (iii) various policy documents provided to GAO as part of this study to describe the agency CIO's role in the responsibilities listed in *Table 1: Summary of Key Chief Information Officer (CIO) Responsibilities.* These documents were developed to empower the CIO to execute all tasks as described in federal law and OMB guidance. The Department's CIO is currently performing most of the responsibilities enumerated in this study. However, we recognize that the responsibilities are not explicitly documented in our policies, and we plan to update these policies to reflect the specific requirements identified by GAO.

400 MARYLAND AVE. S.W., WASHINGTON, DC 20202
www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.



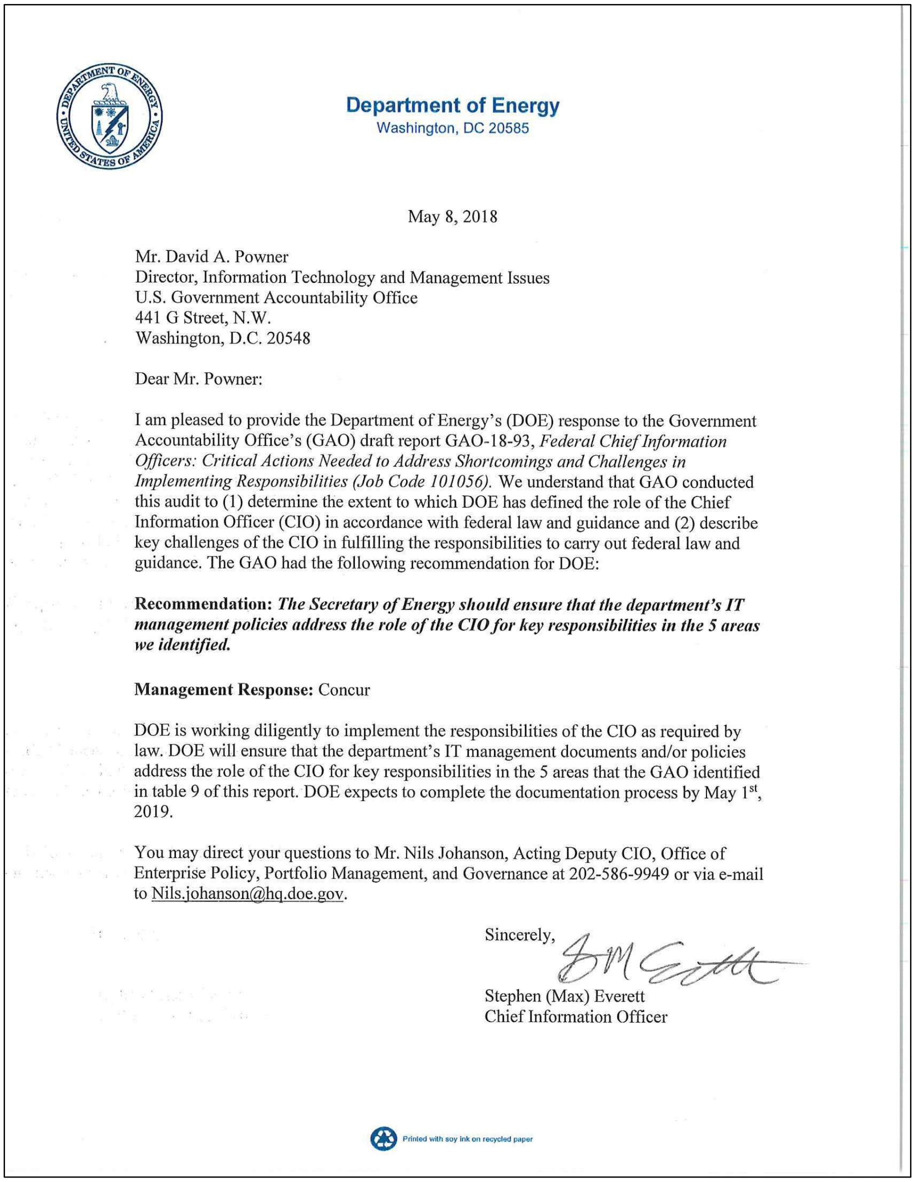
As part of maturing agency policies under our FITARA implementation initiative, the Department is updating and developing agency policies to address the role of the CIO for key responsibilities in the five areas GAO identified and as listed in *Table 8: Extent to Which Department of Education Policies Addressed the Role of Its Chief Information Officer* on pages 60-61 of GAO-18-93.

If you have any questions, please contact Walter McDonald, Director of Information Technology Program Services, at (202) 245-6794 or at Walter.McDonald@ed.gov.

Sincerely,

Jason K. Gray

# Appendix IX: Comments from the Department of Energy



**Department of Energy**
Washington, DC 20585

May 8, 2018

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-18-93, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (Job Code 101056).* We understand that GAO conducted this audit to (1) determine the extent to which DOE has defined the role of the Chief Information Officer (CIO) in accordance with federal law and guidance and (2) describe key challenges of the CIO in fulfilling the responsibilities to carry out federal law and guidance. The GAO had the following recommendation for DOE:

**Recommendation:** ***The Secretary of Energy should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified.***

**Management Response:** Concur

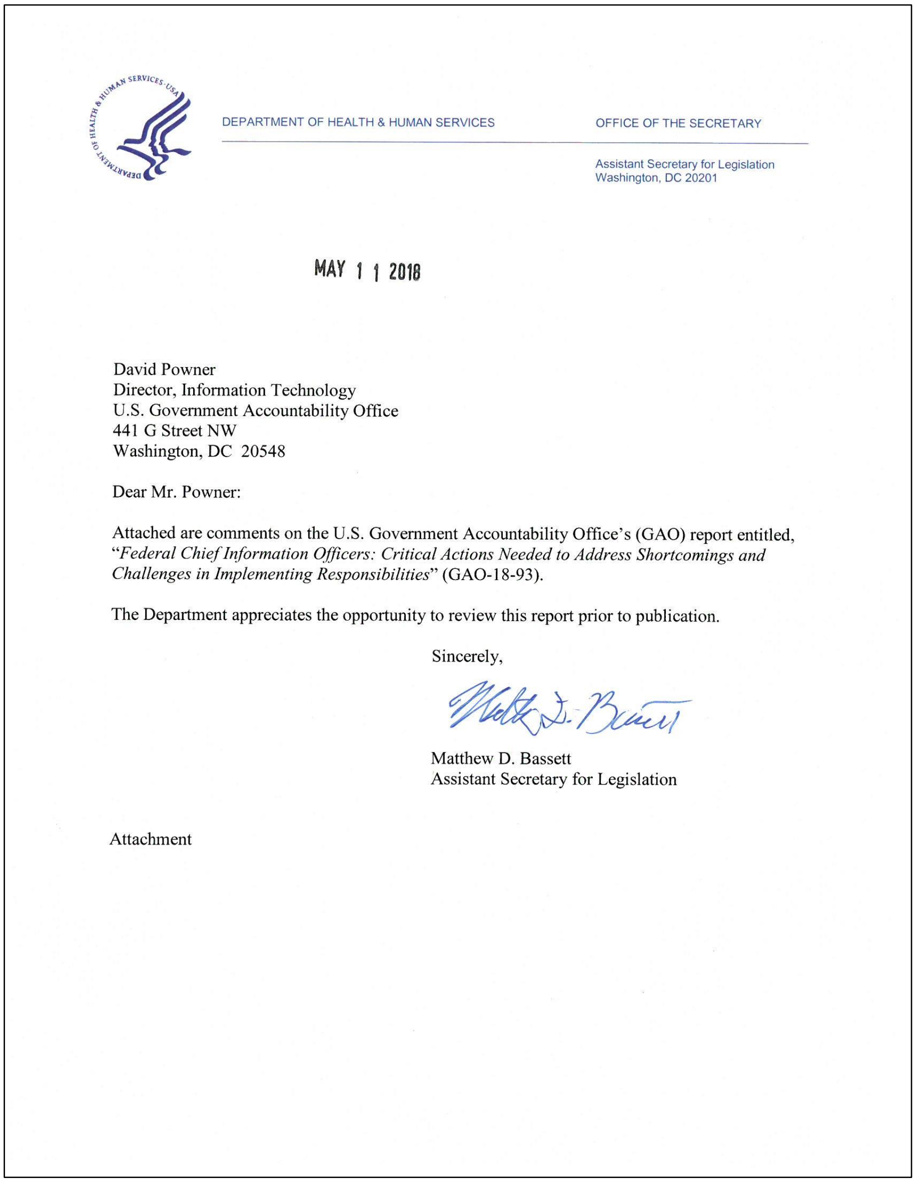
DOE is working diligently to implement the responsibilities of the CIO as required by law. DOE will ensure that the department's IT management documents and/or policies address the role of the CIO for key responsibilities in the 5 areas that the GAO identified in table 9 of this report. DOE expects to complete the documentation process by May 1st, 2019.

You may direct your questions to Mr. Nils Johanson, Acting Deputy CIO, Office of Enterprise Policy, Portfolio Management, and Governance at 202-586-9949 or via e-mail to Nils.johanson@hq.doe.gov.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

# Appendix X: 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

MAY 1 1 2018

David Powner
Director, Information Technology
U.S. Government Accountability Office
441 G Street NW
Washington, DC  20548

Dear Mr. Powner:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*" (GAO-18-93).

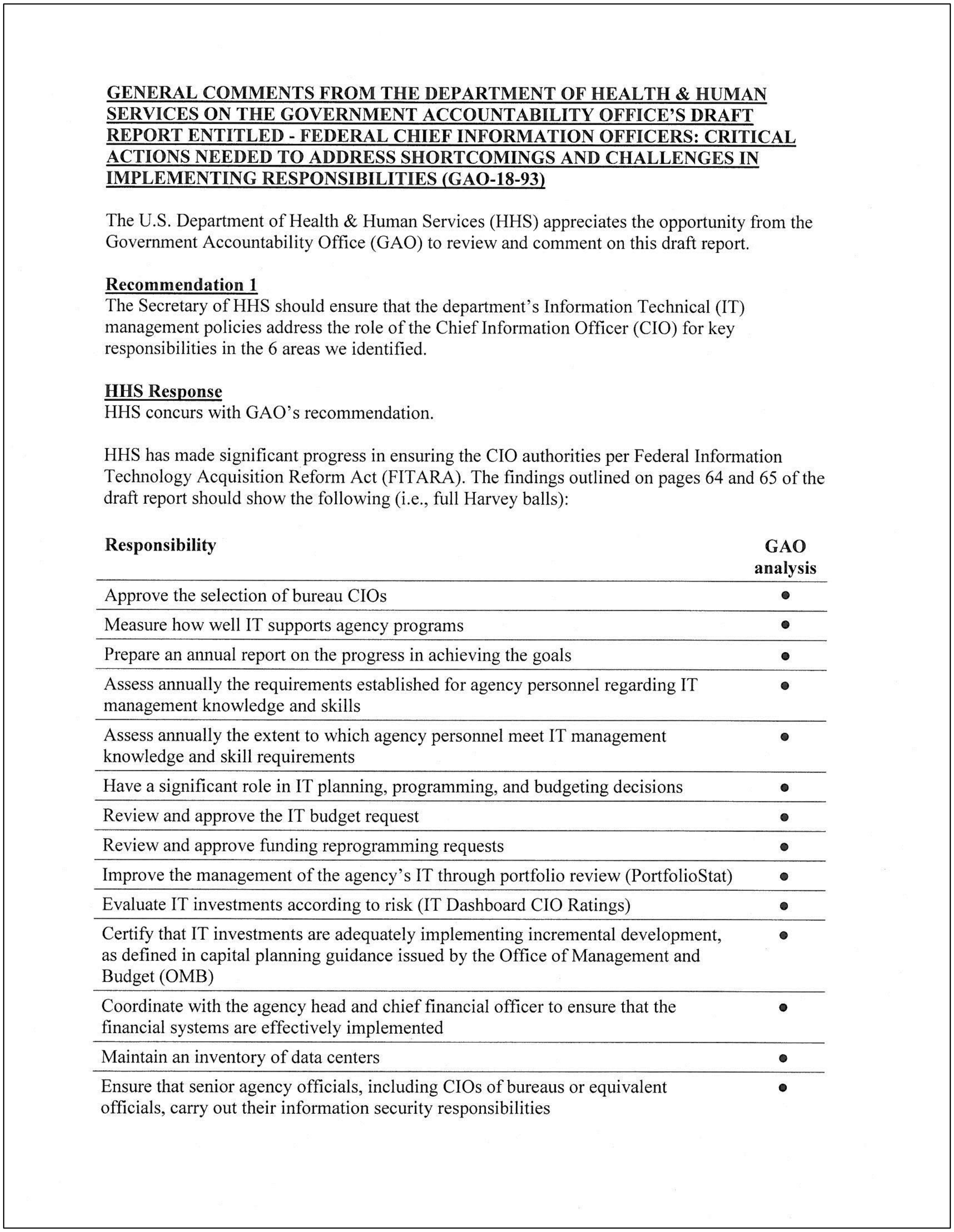
The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Matt D. Bassett

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment



**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)**

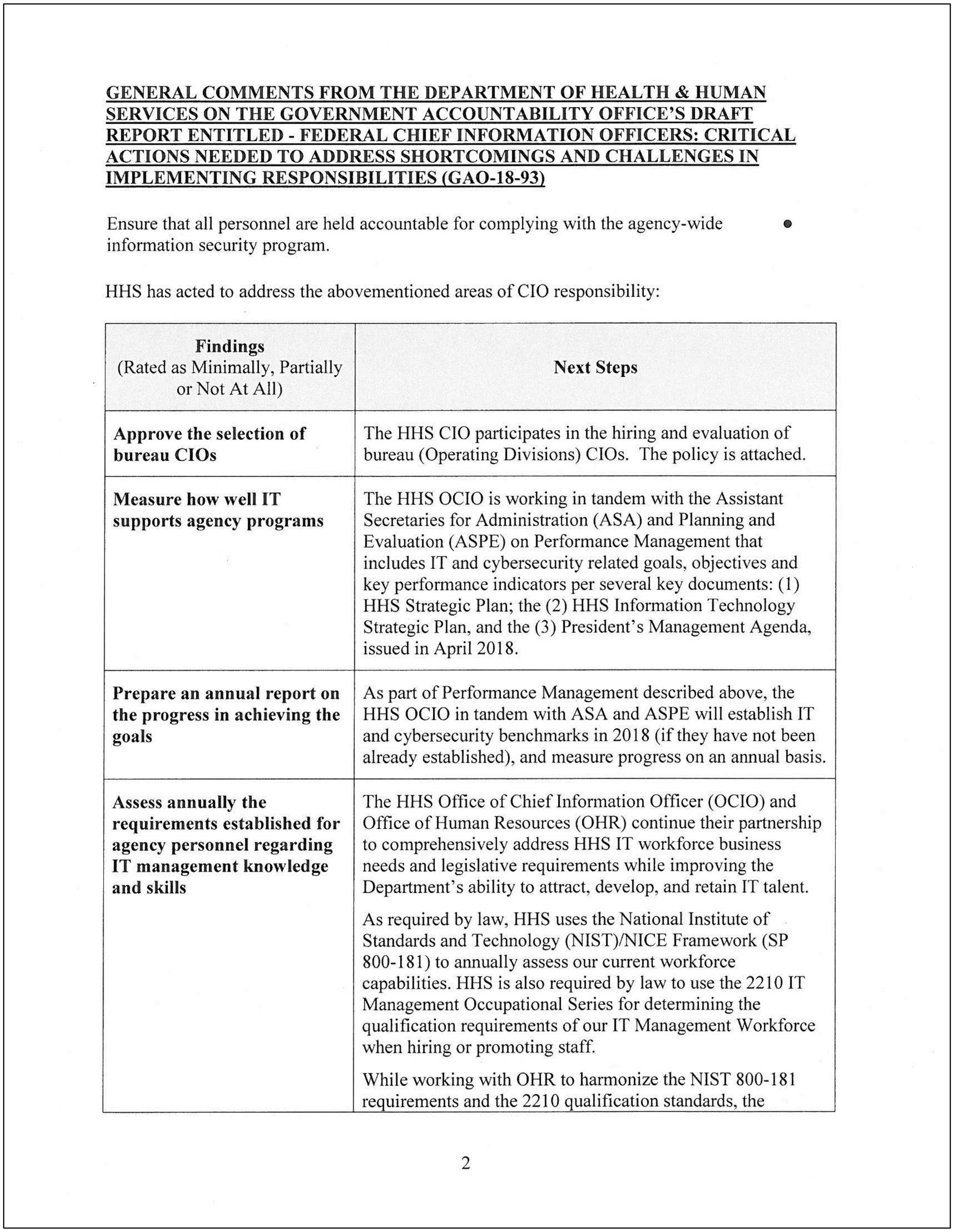
The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

**Recommendation 1**
The Secretary of HHS should ensure that the department's Information Technical (IT) management policies address the role of the Chief Information Officer (CIO) for key responsibilities in the 6 areas we identified.

**HHS Response**
HHS concurs with GAO's recommendation.

HHS has made significant progress in ensuring the CIO authorities per Federal Information Technology Acquisition Reform Act (FITARA). The findings outlined on pages 64 and 65 of the draft report should show the following (i.e., full Harvey balls):

| Responsibility | GAO analysis |
|---|---|
| Approve the selection of bureau CIOs | ● |
| Measure how well IT supports agency programs | ● |
| Prepare an annual report on the progress in achieving the goals | ● |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | ● |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | ● |
| Have a significant role in IT planning, programming, and budgeting decisions | ● |
| Review and approve the IT budget request | ● |
| Review and approve funding reprogramming requests | ● |
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | ● |
| Evaluate IT investments according to risk (IT Dashboard CIO Ratings) | ● |
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget (OMB) | ● |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | ● |
| Maintain an inventory of data centers | ● |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | ● |



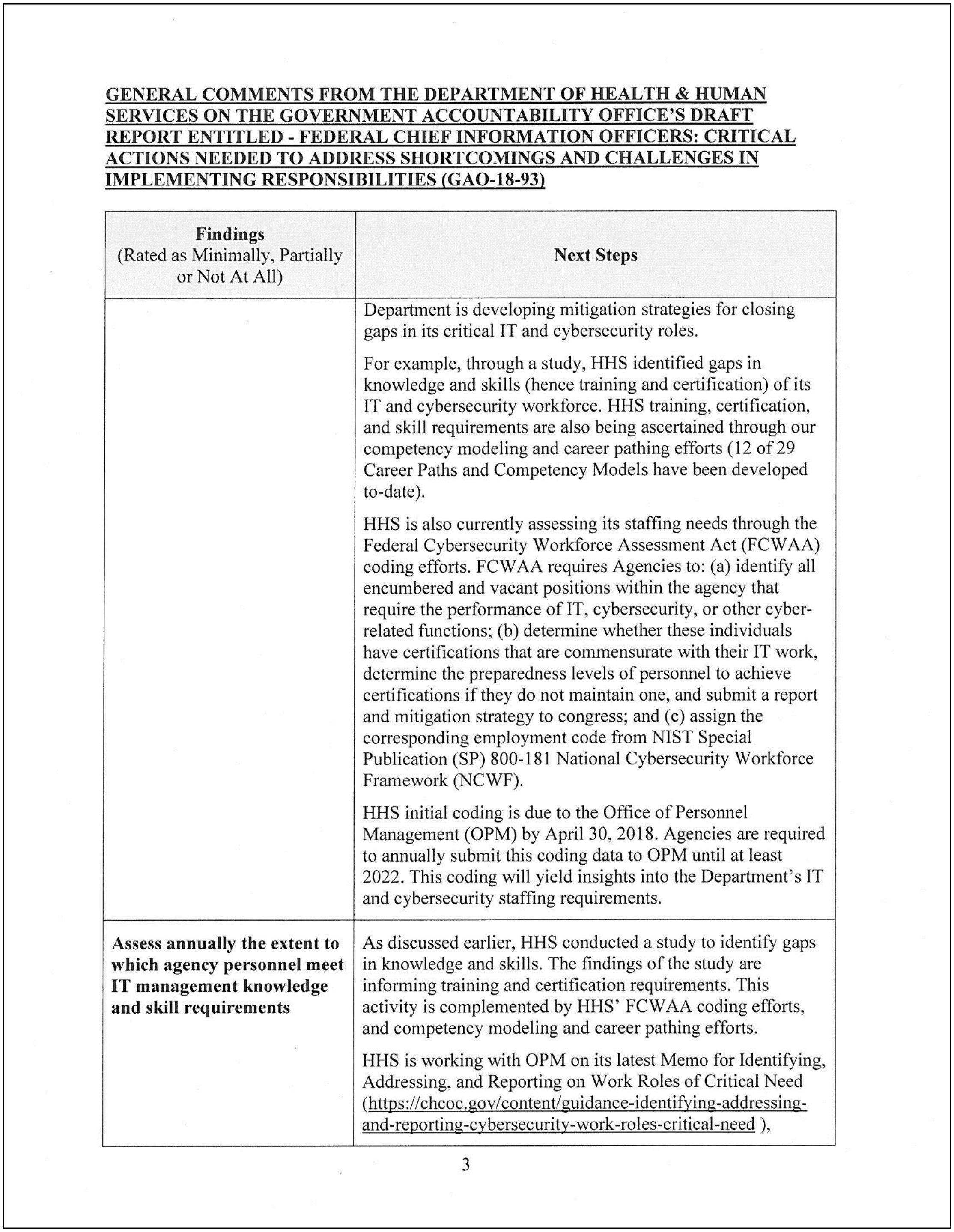
**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)**

Ensure that all personnel are held accountable for complying with the agency-wide information security program. ●

HHS has acted to address the abovementioned areas of CIO responsibility:

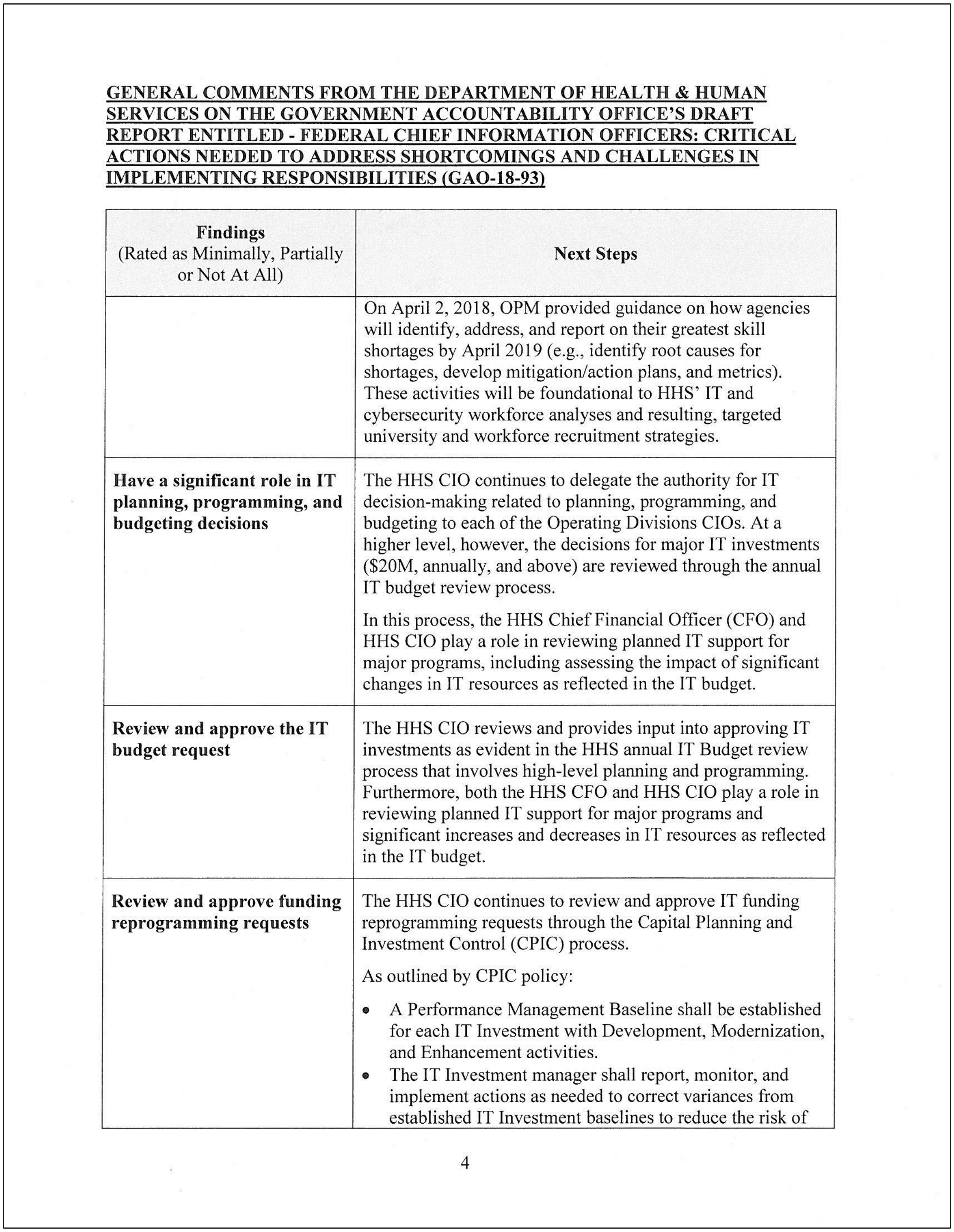
| **Findings**<br>(Rated as Minimally, Partially or Not At All) | **Next Steps** |
|---|---|
| **Approve the selection of bureau CIOs** | The HHS CIO participates in the hiring and evaluation of bureau (Operating Divisions) CIOs. The policy is attached. |
| **Measure how well IT supports agency programs** | The HHS OCIO is working in tandem with the Assistant Secretaries for Administration (ASA) and Planning and Evaluation (ASPE) on Performance Management that includes IT and cybersecurity related goals, objectives and key performance indicators per several key documents: (1) HHS Strategic Plan; the (2) HHS Information Technology Strategic Plan, and the (3) President's Management Agenda, issued in April 2018. |
| **Prepare an annual report on the progress in achieving the goals** | As part of Performance Management described above, the HHS OCIO in tandem with ASA and ASPE will establish IT and cybersecurity benchmarks in 2018 (if they have not been already established), and measure progress on an annual basis. |
| **Assess annually the requirements established for agency personnel regarding IT management knowledge and skills** | The HHS Office of Chief Information Officer (OCIO) and Office of Human Resources (OHR) continue their partnership to comprehensively address HHS IT workforce business needs and legislative requirements while improving the Department's ability to attract, develop, and retain IT talent.<br>As required by law, HHS uses the National Institute of Standards and Technology (NIST)/NICE Framework (SP 800-181) to annually assess our current workforce capabilities. HHS is also required by law to use the 2210 IT Management Occupational Series for determining the qualification requirements of our IT Management Workforce when hiring or promoting staff.<br>While working with OHR to harmonize the NIST 800-181 requirements and the 2210 qualification standards, the |

2



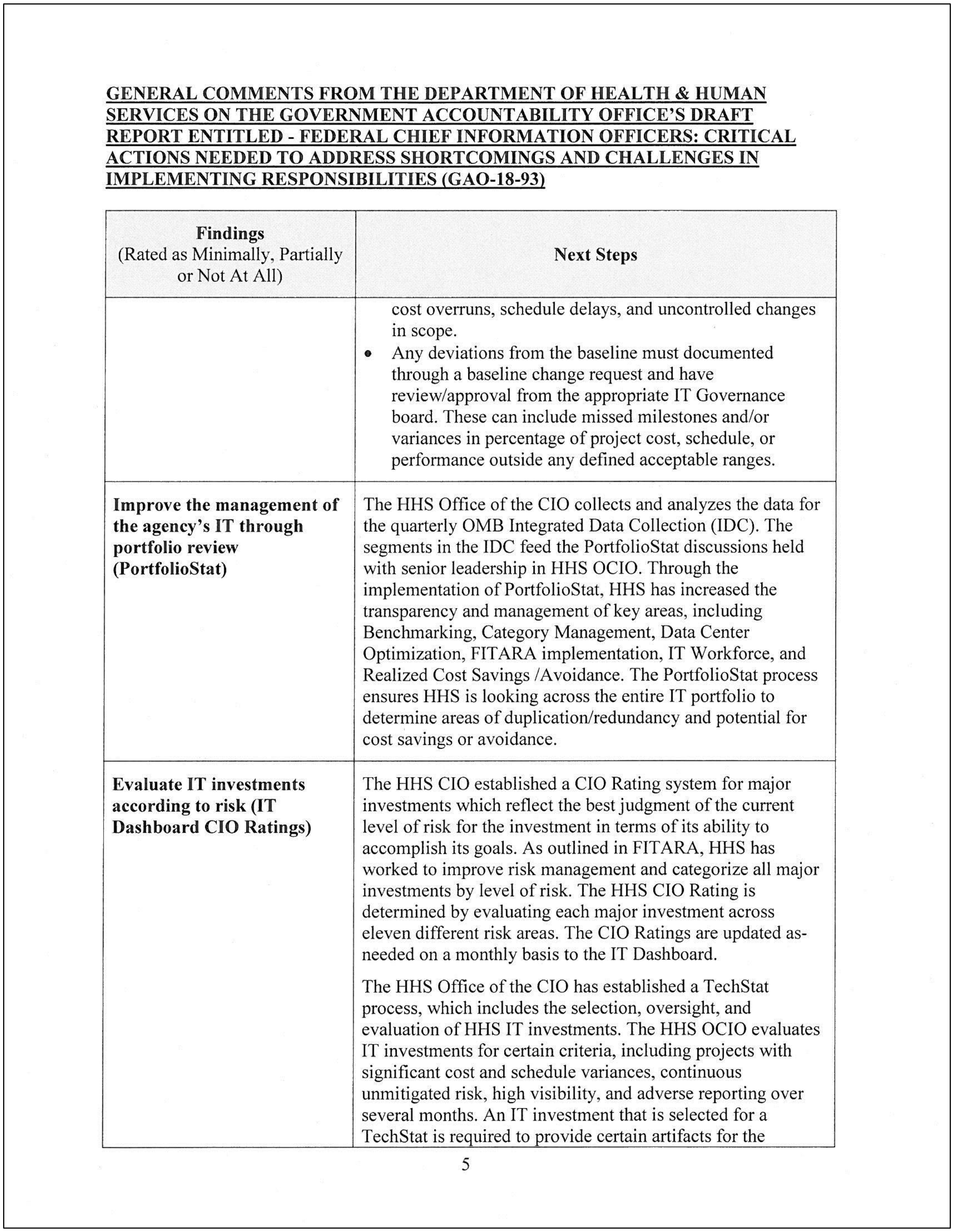
**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)**

| **Findings**<br>(Rated as Minimally, Partially or Not At All) | **Next Steps** |
|---|---|
| | Department is developing mitigation strategies for closing gaps in its critical IT and cybersecurity roles.<br>For example, through a study, HHS identified gaps in knowledge and skills (hence training and certification) of its IT and cybersecurity workforce. HHS training, certification, and skill requirements are also being ascertained through our competency modeling and career pathing efforts (12 of 29 Career Paths and Competency Models have been developed to-date).<br>HHS is also currently assessing its staffing needs through the Federal Cybersecurity Workforce Assessment Act (FCWAA) coding efforts. FCWAA requires Agencies to: (a) identify all encumbered and vacant positions within the agency that require the performance of IT, cybersecurity, or other cyber-related functions; (b) determine whether these individuals have certifications that are commensurate with their IT work, determine the preparedness levels of personnel to achieve certifications if they do not maintain one, and submit a report and mitigation strategy to congress; and (c) assign the corresponding employment code from NIST Special Publication (SP) 800-181 National Cybersecurity Workforce Framework (NCWF).<br>HHS initial coding is due to the Office of Personnel Management (OPM) by April 30, 2018. Agencies are required to annually submit this coding data to OPM until at least 2022. This coding will yield insights into the Department's IT and cybersecurity staffing requirements. |
| **Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements** | As discussed earlier, HHS conducted a study to identify gaps in knowledge and skills. The findings of the study are informing training and certification requirements. This activity is complemented by HHS' FCWAA coding efforts, and competency modeling and career pathing efforts.<br>HHS is working with OPM on its latest Memo for Identifying, Addressing, and Reporting on Work Roles of Critical Need (https://chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need ), |



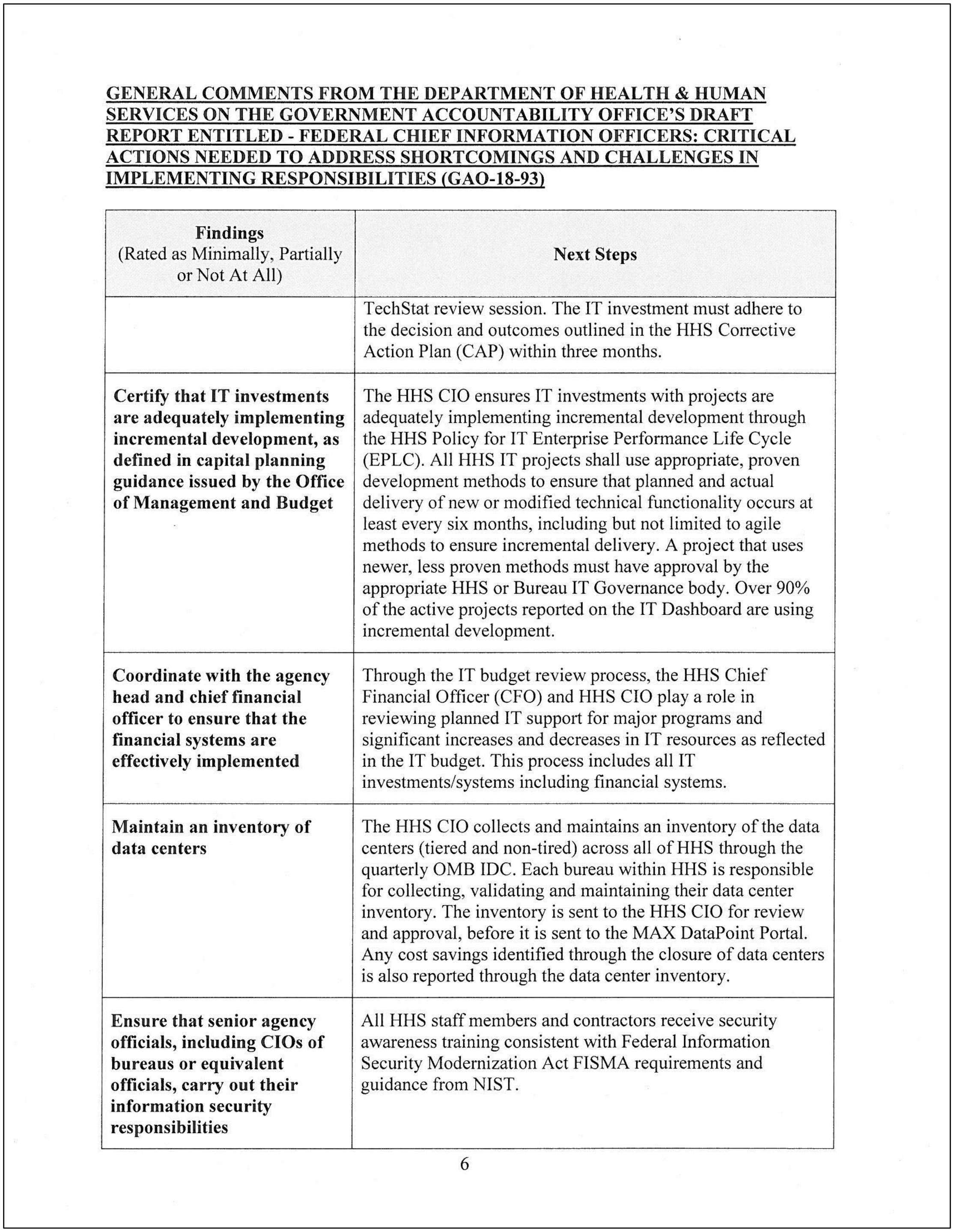
**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)**

| **Findings**<br>(Rated as Minimally, Partially or Not At All) | **Next Steps** |
|---|---|
| | On April 2, 2018, OPM provided guidance on how agencies will identify, address, and report on their greatest skill shortages by April 2019 (e.g., identify root causes for shortages, develop mitigation/action plans, and metrics). These activities will be foundational to HHS' IT and cybersecurity workforce analyses and resulting, targeted university and workforce recruitment strategies. |
| **Have a significant role in IT planning, programming, and budgeting decisions** | The HHS CIO continues to delegate the authority for IT decision-making related to planning, programming, and budgeting to each of the Operating Divisions CIOs. At a higher level, however, the decisions for major IT investments ($20M, annually, and above) are reviewed through the annual IT budget review process.<br>In this process, the HHS Chief Financial Officer (CFO) and HHS CIO play a role in reviewing planned IT support for major programs, including assessing the impact of significant changes in IT resources as reflected in the IT budget. |
| **Review and approve the IT budget request** | The HHS CIO reviews and provides input into approving IT investments as evident in the HHS annual IT Budget review process that involves high-level planning and programming. Furthermore, both the HHS CFO and HHS CIO play a role in reviewing planned IT support for major programs and significant increases and decreases in IT resources as reflected in the IT budget. |
| **Review and approve funding reprogramming requests** | The HHS CIO continues to review and approve IT funding reprogramming requests through the Capital Planning and Investment Control (CPIC) process.<br>As outlined by CPIC policy:<br>• A Performance Management Baseline shall be established for each IT Investment with Development, Modernization, and Enhancement activities.<br>• The IT Investment manager shall report, monitor, and implement actions as needed to correct variances from established IT Investment baselines to reduce the risk of |



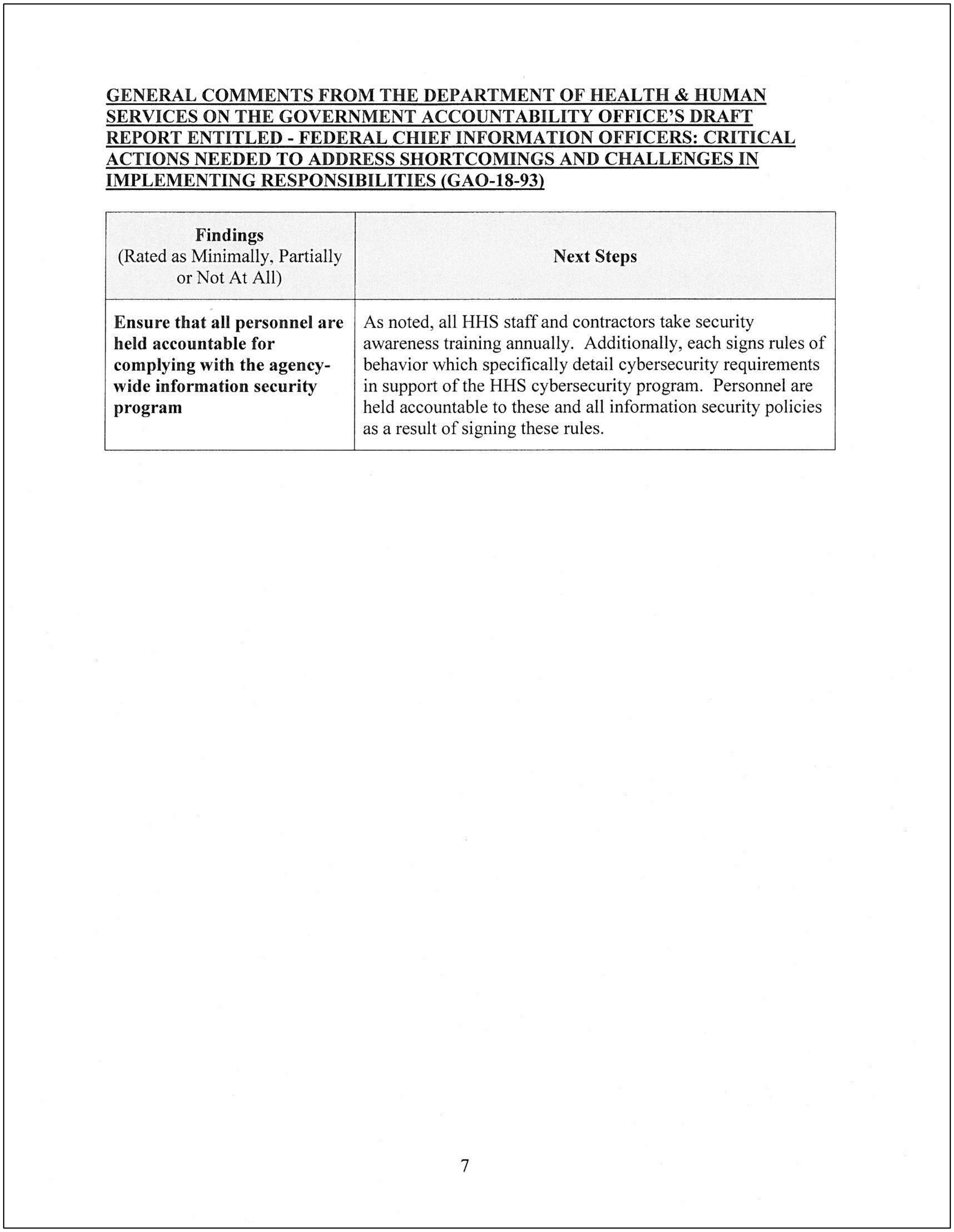
**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)**

| **Findings**<br>(Rated as Minimally, Partially or Not At All) | **Next Steps** |
|---|---|
| | cost overruns, schedule delays, and uncontrolled changes in scope.<br>• Any deviations from the baseline must documented through a baseline change request and have review/approval from the appropriate IT Governance board. These can include missed milestones and/or variances in percentage of project cost, schedule, or performance outside any defined acceptable ranges. |
| **Improve the management of the agency's IT through portfolio review (PortfolioStat)** | The HHS Office of the CIO collects and analyzes the data for the quarterly OMB Integrated Data Collection (IDC). The segments in the IDC feed the PortfolioStat discussions held with senior leadership in HHS OCIO. Through the implementation of PortfolioStat, HHS has increased the transparency and management of key areas, including Benchmarking, Category Management, Data Center Optimization, FITARA implementation, IT Workforce, and Realized Cost Savings /Avoidance. The PortfolioStat process ensures HHS is looking across the entire IT portfolio to determine areas of duplication/redundancy and potential for cost savings or avoidance. |
| **Evaluate IT investments according to risk (IT Dashboard CIO Ratings)** | The HHS CIO established a CIO Rating system for major investments which reflect the best judgment of the current level of risk for the investment in terms of its ability to accomplish its goals. As outlined in FITARA, HHS has worked to improve risk management and categorize all major investments by level of risk. The HHS CIO Rating is determined by evaluating each major investment across eleven different risk areas. The CIO Ratings are updated as-needed on a monthly basis to the IT Dashboard.<br>The HHS Office of the CIO has established a TechStat process, which includes the selection, oversight, and evaluation of HHS IT investments. The HHS OCIO evaluates IT investments for certain criteria, including projects with significant cost and schedule variances, continuous unmitigated risk, high visibility, and adverse reporting over several months. An IT investment that is selected for a TechStat is required to provide certain artifacts for the |



**GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)**

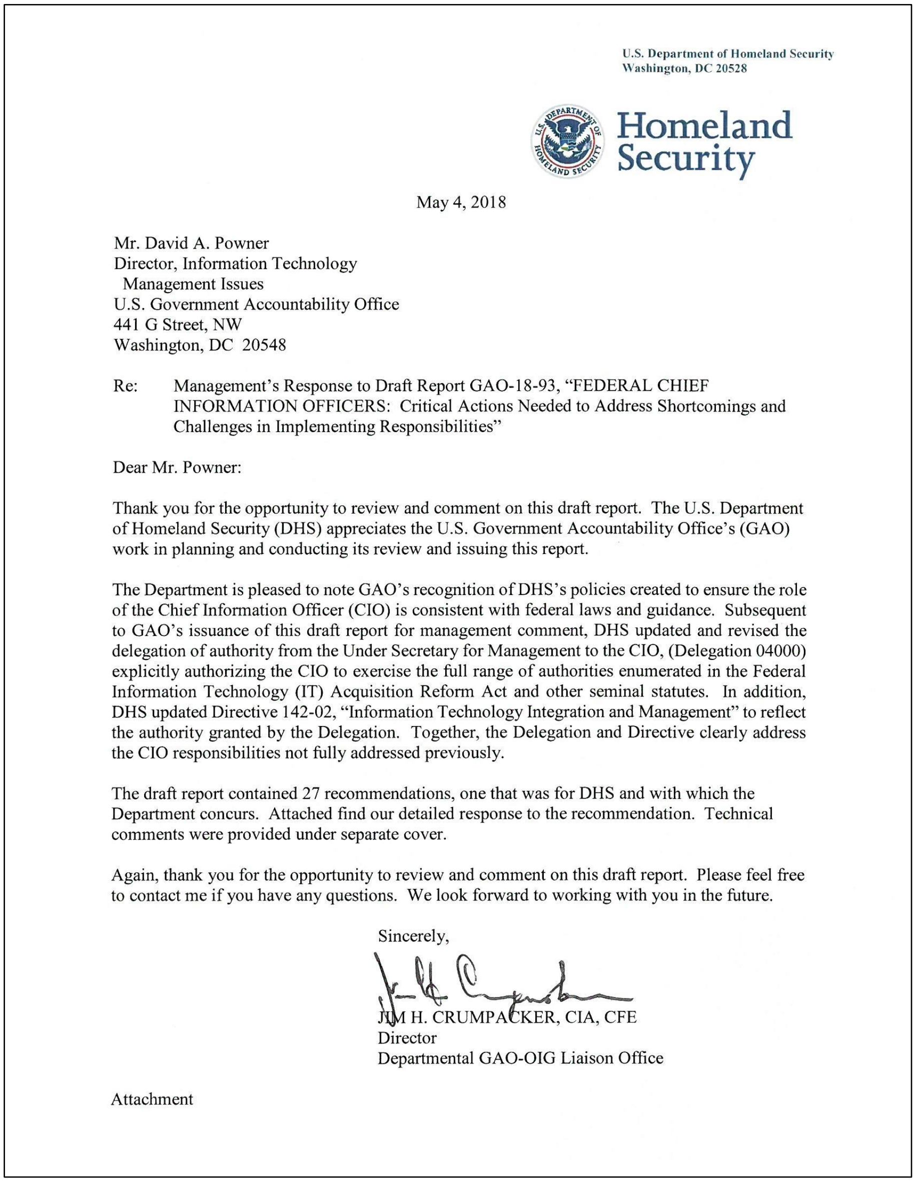
| **Findings**<br>(Rated as Minimally, Partially or Not At All) | **Next Steps** |
|---|---|
| | TechStat review session. The IT investment must adhere to the decision and outcomes outlined in the HHS Corrective Action Plan (CAP) within three months. |
| **Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget** | The HHS CIO ensures IT investments with projects are adequately implementing incremental development through the HHS Policy for IT Enterprise Performance Life Cycle (EPLC). All HHS IT projects shall use appropriate, proven development methods to ensure that planned and actual delivery of new or modified technical functionality occurs at least every six months, including but not limited to agile methods to ensure incremental delivery. A project that uses newer, less proven methods must have approval by the appropriate HHS or Bureau IT Governance body. Over 90% of the active projects reported on the IT Dashboard are using incremental development. |
| **Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented** | Through the IT budget review process, the HHS Chief Financial Officer (CFO) and HHS CIO play a role in reviewing planned IT support for major programs and significant increases and decreases in IT resources as reflected in the IT budget. This process includes all IT investments/systems including financial systems. |
| **Maintain an inventory of data centers** | The HHS CIO collects and maintains an inventory of the data centers (tiered and non-tiered) across all of HHS through the quarterly OMB IDC. Each bureau within HHS is responsible for collecting, validating and maintaining their data center inventory. The inventory is sent to the HHS CIO for review and approval, before it is sent to the MAX DataPoint Portal. Any cost savings identified through the closure of data centers is also reported through the data center inventory. |
| **Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities** | All HHS staff members and contractors receive security awareness training consistent with Federal Information Security Modernization Act FISMA requirements and guidance from NIST. |



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES (GAO-18-93)

| **Findings**<br>(Rated as Minimally, Partially or Not At All) | **Next Steps** |
|---|---|
| **Ensure that all personnel are held accountable for complying with the agency-wide information security program** | As noted, all HHS staff and contractors take security awareness training annually. Additionally, each signs rules of behavior which specifically detail cybersecurity requirements in support of the HHS cybersecurity program. Personnel are held accountable to these and all information security policies as a result of signing these rules. |

# Appendix XI: Comments from the Department of Homeland Security



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

Homeland Security

May 4, 2018

Mr. David A. Powner
Director, Information Technology
Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-18-93, "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities"

Dear Mr. Powner:

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

The Department is pleased to note GAO's recognition of DHS's policies created to ensure the role of the Chief Information Officer (CIO) is consistent with federal laws and guidance. Subsequent to GAO's issuance of this draft report for management comment, DHS updated and revised the delegation of authority from the Under Secretary for Management to the CIO, (Delegation 04000) explicitly authorizing the CIO to exercise the full range of authorities enumerated in the Federal Information Technology (IT) Acquisition Reform Act and other seminal statutes. In addition, DHS updated Directive 142-02, "Information Technology Integration and Management" to reflect the authority granted by the Delegation. Together, the Delegation and Directive clearly address the CIO responsibilities not fully addressed previously.

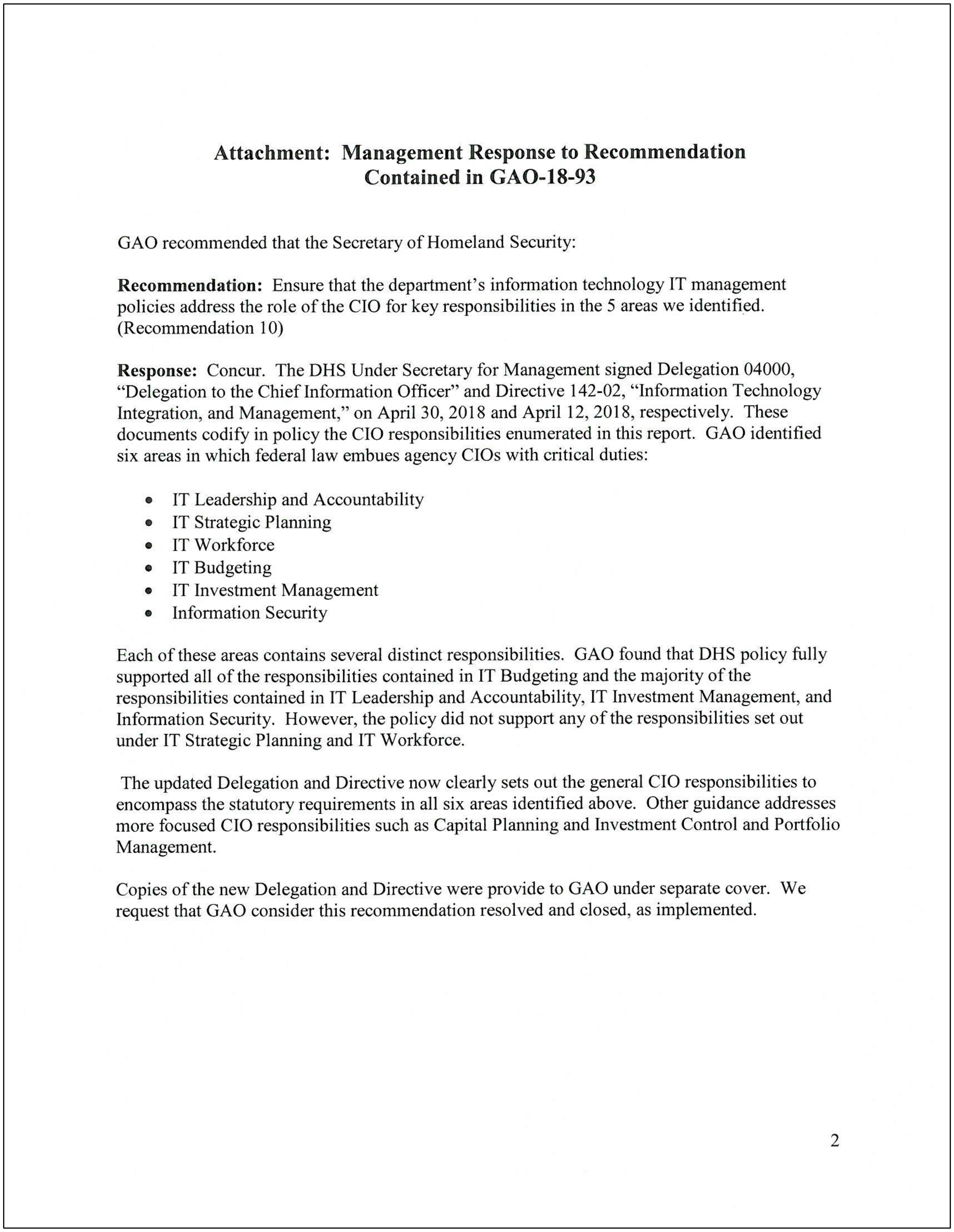
The draft report contained 27 recommendations, one that was for DHS and with which the Department concurs. Attached find our detailed response to the recommendation. Technical comments were provided under separate cover.

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

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment



## Attachment: Management Response to Recommendation Contained in GAO-18-93

GAO recommended that the Secretary of Homeland Security:

**Recommendation:** Ensure that the department's information technology IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified. (Recommendation 10)

**Response:** Concur. The DHS Under Secretary for Management signed Delegation 04000, "Delegation to the Chief Information Officer" and Directive 142-02, "Information Technology Integration, and Management," on April 30, 2018 and April 12, 2018, respectively. These documents codify in policy the CIO responsibilities enumerated in this report. GAO identified six areas in which federal law embues agency CIOs with critical duties:

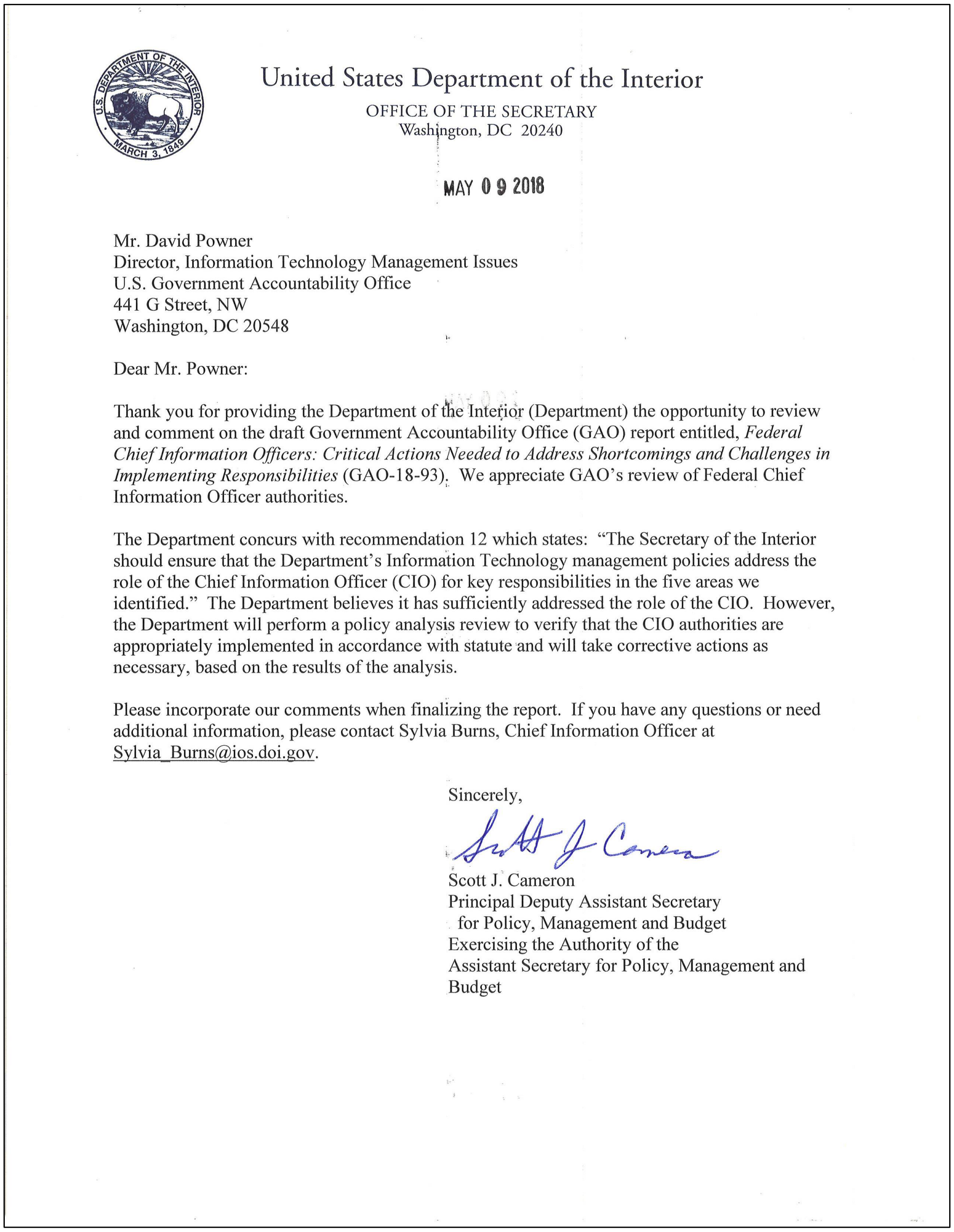
- IT Leadership and Accountability
- IT Strategic Planning
- IT Workforce
- IT Budgeting
- IT Investment Management
- Information Security

Each of these areas contains several distinct responsibilities. GAO found that DHS policy fully supported all of the responsibilities contained in IT Budgeting and the majority of the responsibilities contained in IT Leadership and Accountability, IT Investment Management, and Information Security. However, the policy did not support any of the responsibilities set out under IT Strategic Planning and IT Workforce.

The updated Delegation and Directive now clearly sets out the general CIO responsibilities to encompass the statutory requirements in all six areas identified above. Other guidance addresses more focused CIO responsibilities such as Capital Planning and Investment Control and Portfolio Management.

Copies of the new Delegation and Directive were provide to GAO under separate cover. We request that GAO consider this recommendation resolved and closed, as implemented.

# Appendix XII: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

MAY 09 2018

Mr. David Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

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 Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* (GAO-18-93). We appreciate GAO's review of Federal Chief Information Officer authorities.

The Department concurs with recommendation 12 which states: "The Secretary of the Interior should ensure that the Department's Information Technology management policies address the role of the Chief Information Officer (CIO) for key responsibilities in the five areas we identified." The Department believes it has sufficiently addressed the role of the CIO. However, the Department will perform a policy analysis review to verify that the CIO authorities are appropriately implemented in accordance with statute and will take corrective actions as necessary, based on the results of the analysis.

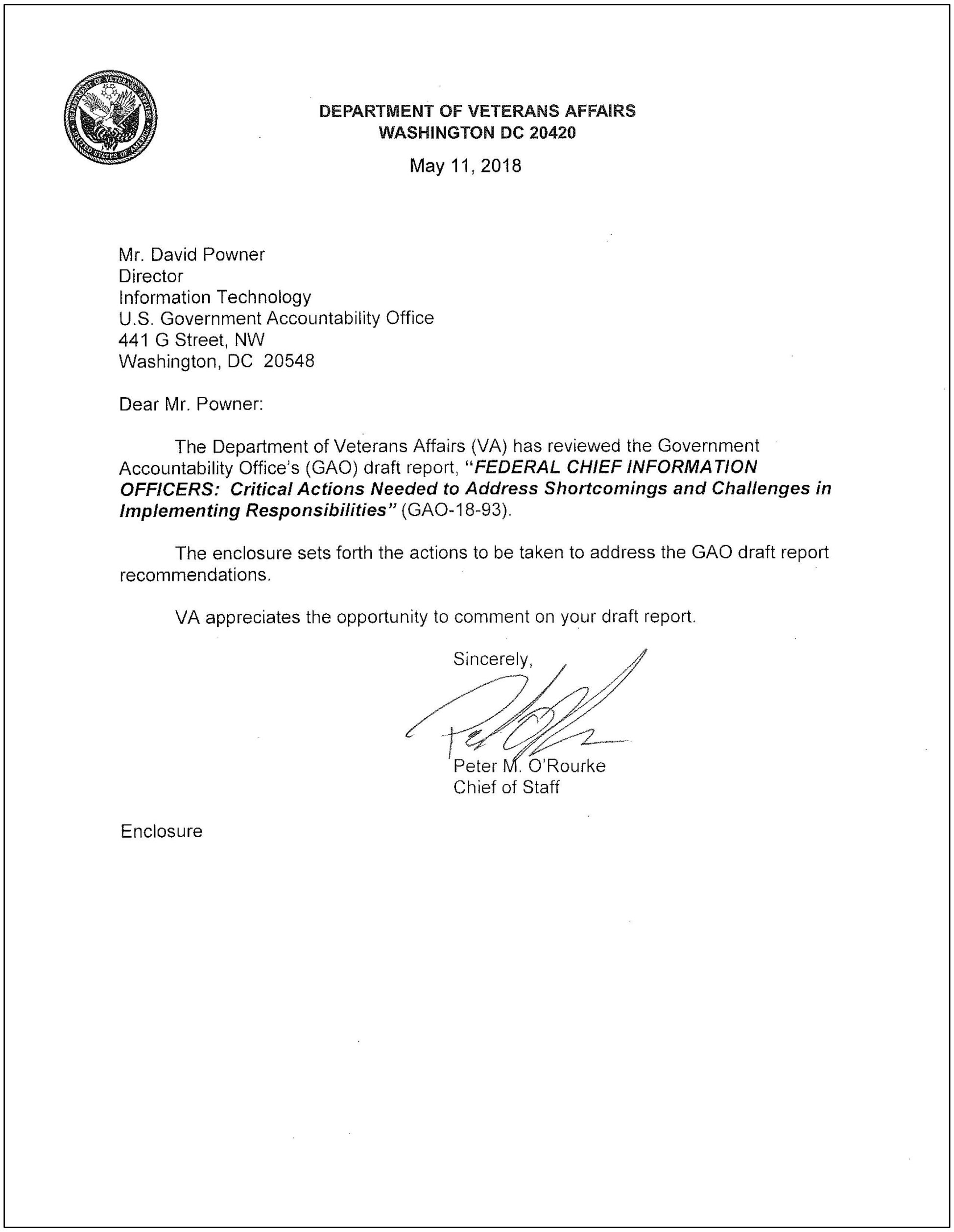
Please incorporate our comments when finalizing the report. If you have any questions or need additional information, please contact Sylvia Burns, Chief Information Officer at Sylvia_Burns@ios.doi.gov.

Sincerely,

Scott J Cameron

Scott J. Cameron
Principal Deputy Assistant Secretary
for Policy, Management and Budget
Exercising the Authority of the
Assistant Secretary for Policy, Management and
Budget

# Appendix XIII: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON DC 20420

May 11, 2018

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

Dear Mr. Powner:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, ***"FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities"*** (GAO-18-93).

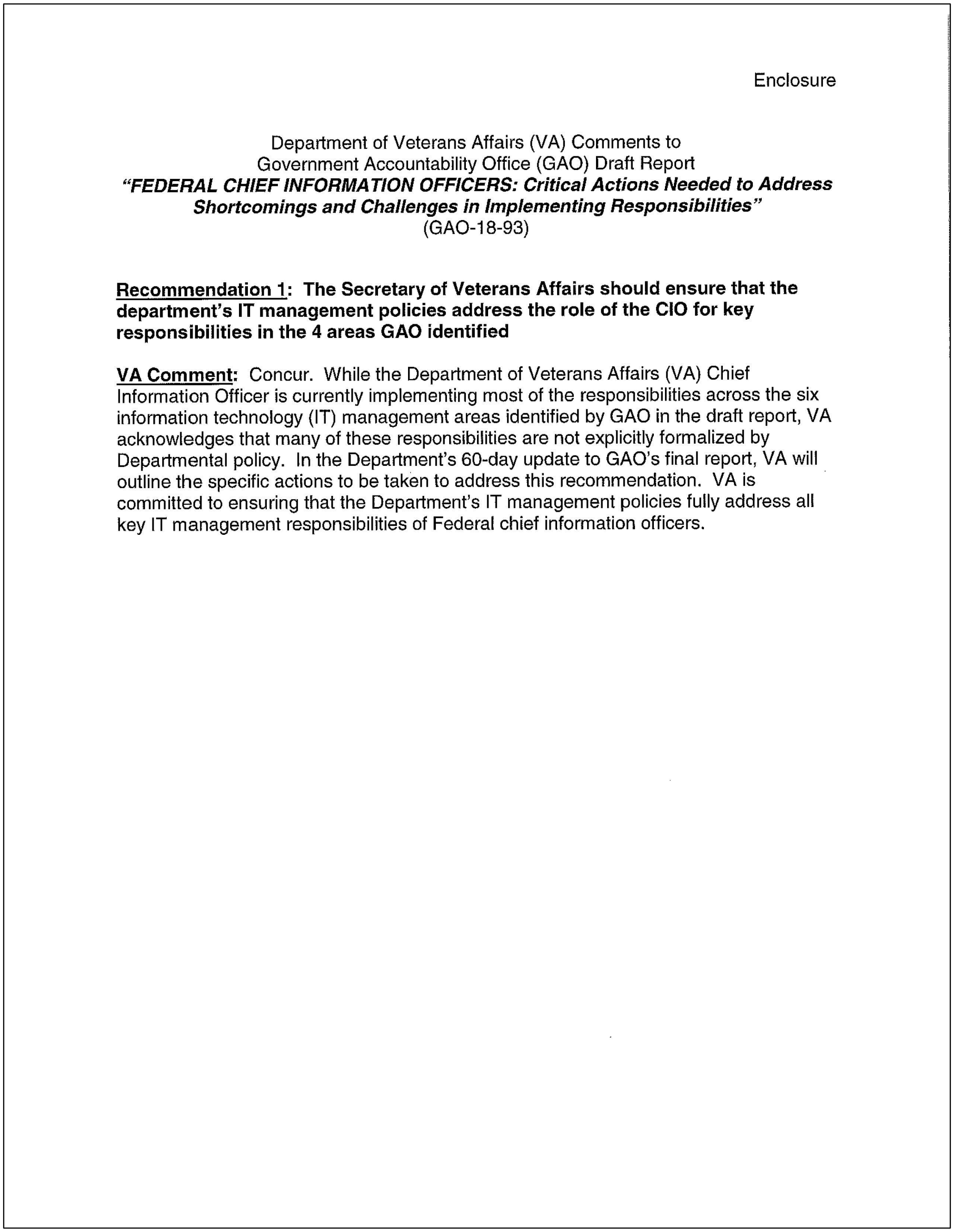
The enclosure sets forth the actions to be taken to address the GAO draft report recommendations.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Peter M. O'Rourke
Chief of Staff

Enclosure



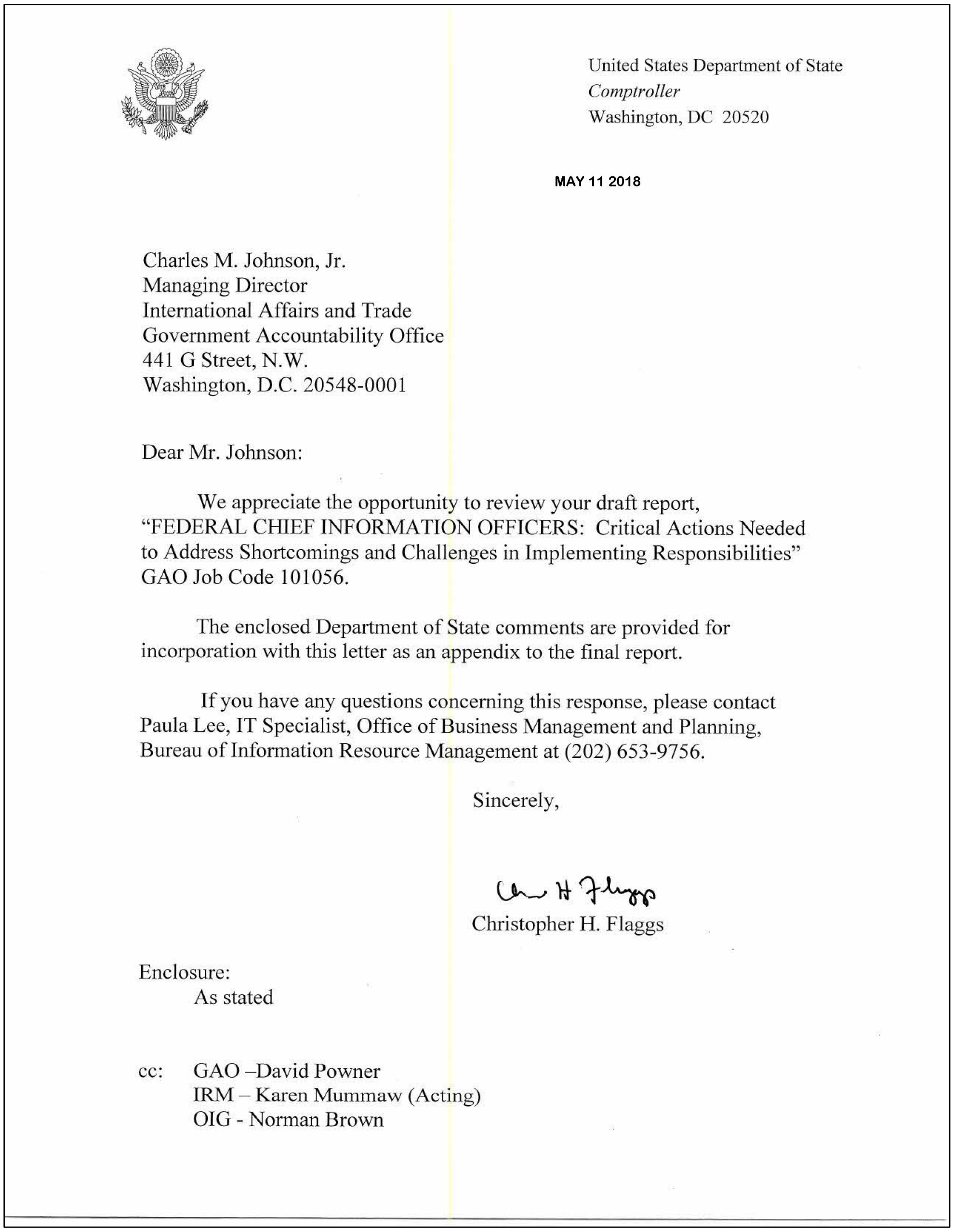
Enclosure

Department of Veterans Affairs (VA) Comments to
Government Accountability Office (GAO) Draft Report
***"FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities"***
(GAO-18-93)

**Recommendation 1: The Secretary of Veterans Affairs should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 4 areas GAO identified**

**VA Comment:** Concur. While the Department of Veterans Affairs (VA) Chief Information Officer is currently implementing most of the responsibilities across the six information technology (IT) management areas identified by GAO in the draft report, VA acknowledges that many of these responsibilities are not explicitly formalized by Departmental policy. In the Department's 60-day update to GAO's final report, VA will outline the specific actions to be taken to address this recommendation. VA is committed to ensuring that the Department's IT management policies fully address all key IT management responsibilities of Federal chief information officers.

# Appendix XIV: Comments from the Department of State



United States Department of State
*Comptroller*
Washington, DC 20520

MAY 11 2018

Charles M. Johnson, Jr.
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Johnson:

We appreciate the opportunity to review your draft report, "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" GAO Job Code 101056.

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

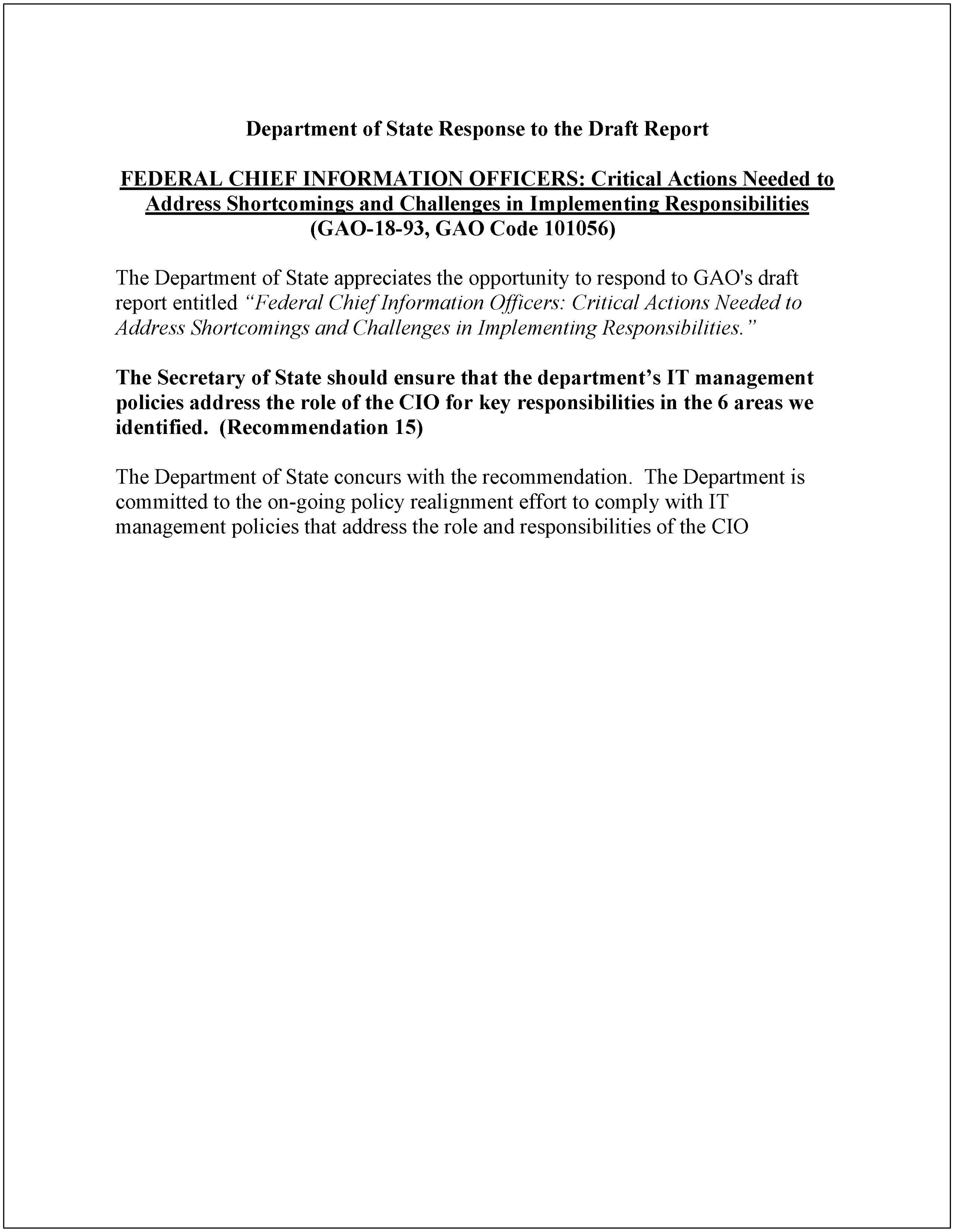
If you have any questions concerning this response, please contact Paula Lee, IT Specialist, Office of Business Management and Planning, Bureau of Information Resource Management at (202) 653-9756.

Sincerely,

Chr H Flaggs
Christopher H. Flaggs

Enclosure:
As stated

cc: GAO –David Powner
IRM – Karen Mummaw (Acting)
OIG - Norman Brown



**Department of State Response to the Draft Report**

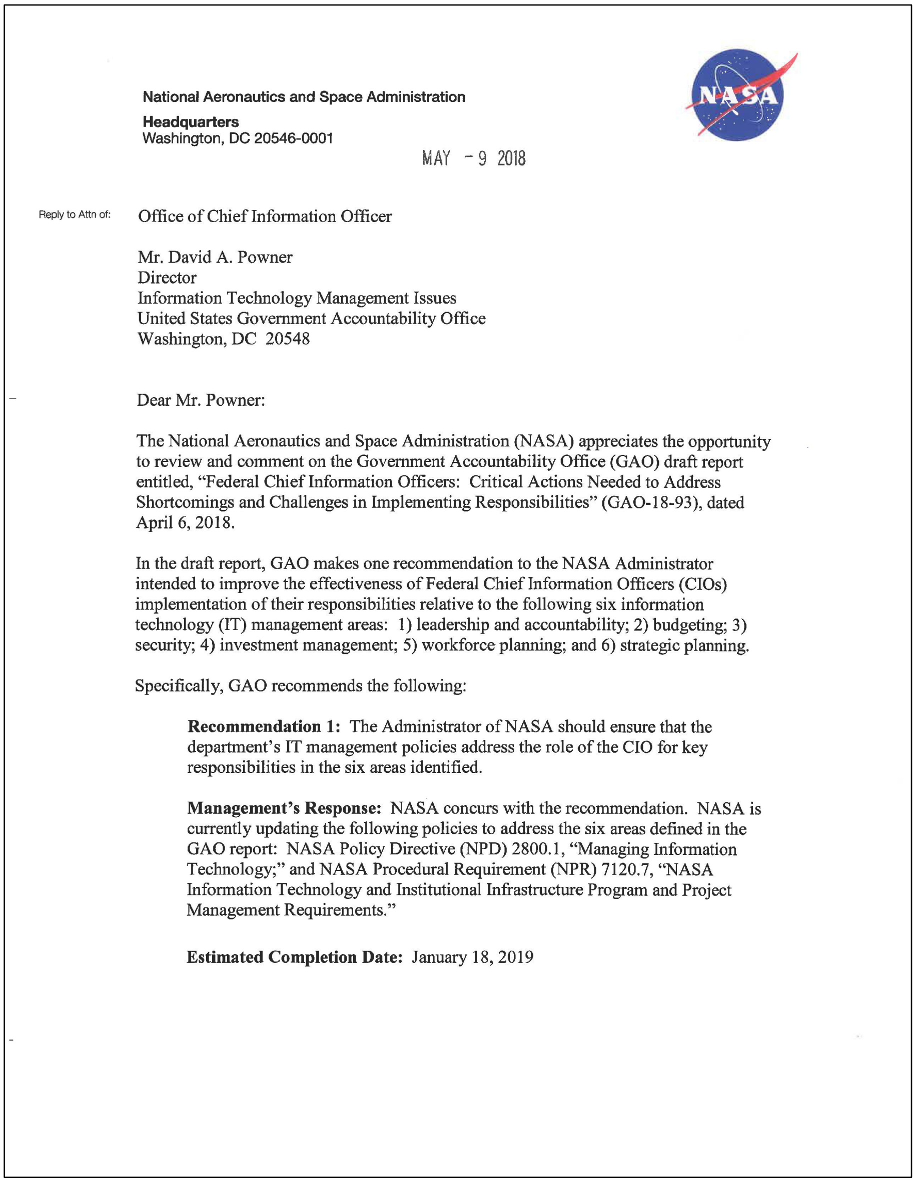
**FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities**
**(GAO-18-93, GAO Code 101056)**

The Department of State appreciates the opportunity to respond to GAO's draft report entitled *"Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities."*

**The Secretary of State should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 6 areas we identified. (Recommendation 15)**

The Department of State concurs with the recommendation. The Department is committed to the on-going policy realignment effort to comply with IT management policies that address the role and responsibilities of the CIO

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



National Aeronautics and Space Administration
**Headquarters**
Washington, DC 20546-0001

MAY - 9 2018

Reply to Attn of: Office of Chief Information Officer

Mr. David A. Powner
Director
Information Technology Management Issues
United States Government Accountability Office
Washington, DC 20548

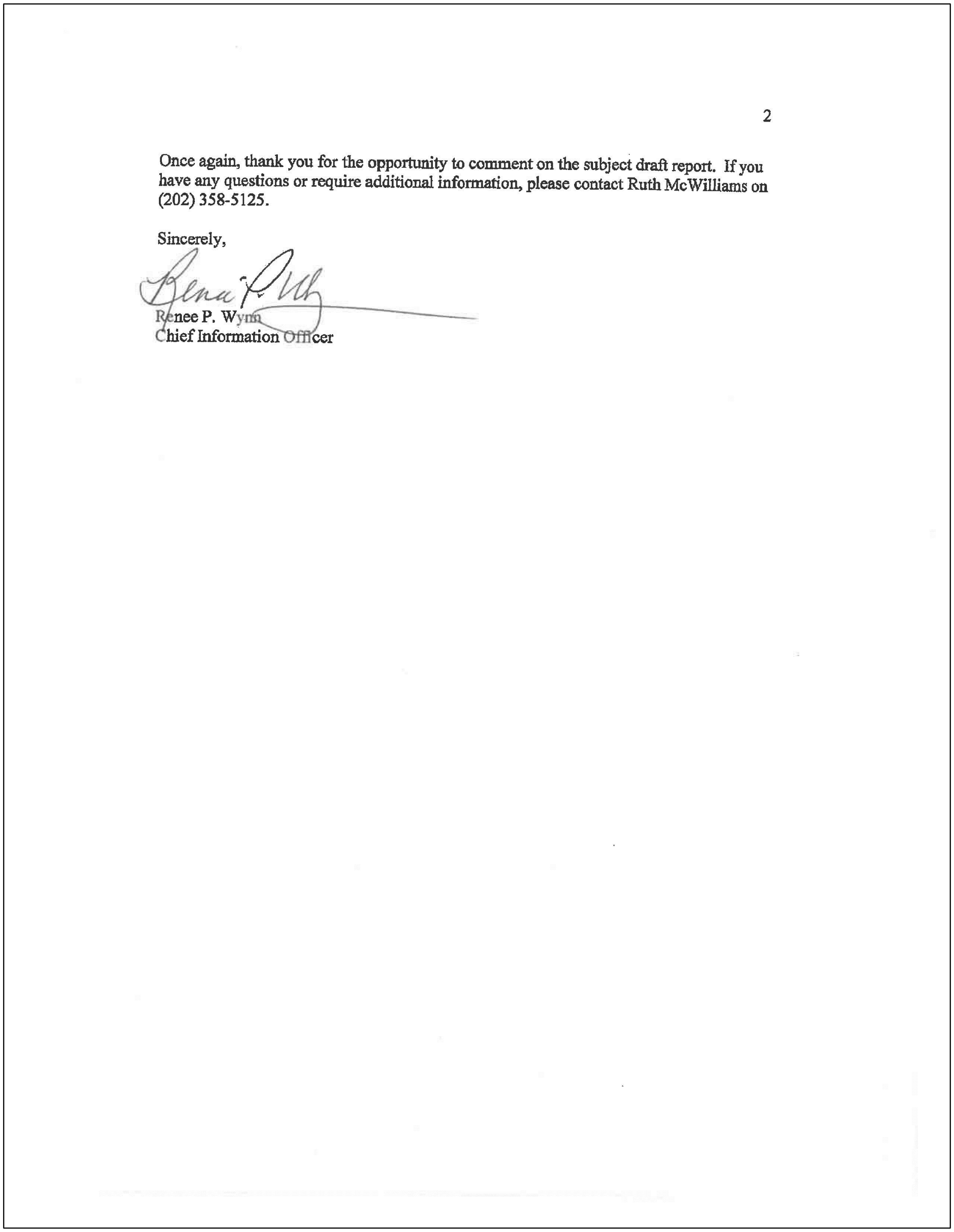
Dear Mr. Powner:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" (GAO-18-93), dated April 6, 2018.

In the draft report, GAO makes one recommendation to the NASA Administrator intended to improve the effectiveness of Federal Chief Information Officers (CIOs) implementation of their responsibilities relative to the following six information technology (IT) management areas: 1) leadership and accountability; 2) budgeting; 3) security; 4) investment management; 5) workforce planning; and 6) strategic planning.

Specifically, GAO recommends the following:

> **Recommendation 1:** The Administrator of NASA should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the six areas identified.
>
> **Management's Response:** NASA concurs with the recommendation. NASA is currently updating the following policies to address the six areas defined in the GAO report: NASA Policy Directive (NPD) 2800.1, "Managing Information Technology;" and NASA Procedural Requirement (NPR) 7120.7, "NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements."
>
> **Estimated Completion Date:** January 18, 2019



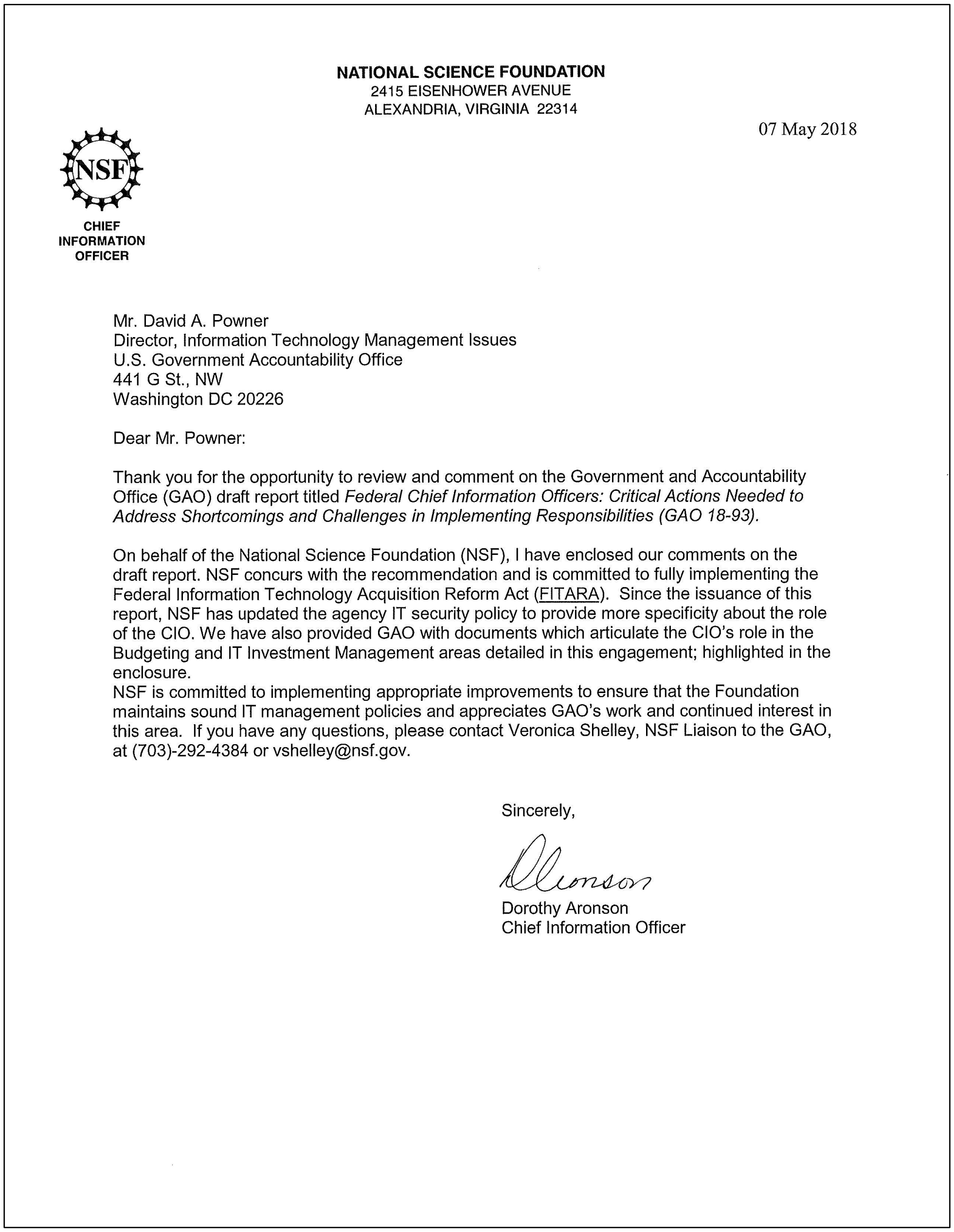
2

Once again, thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Ruth McWilliams on (202) 358-5125.

Sincerely,

Renee P. Wynn
Chief Information Officer

# Appendix XVI: Comments from the National Science Foundation



**NATIONAL SCIENCE FOUNDATION**
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

07 May 2018

CHIEF
INFORMATION
OFFICER

Mr. David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G St., NW
Washington DC 20226

Dear Mr. Powner:

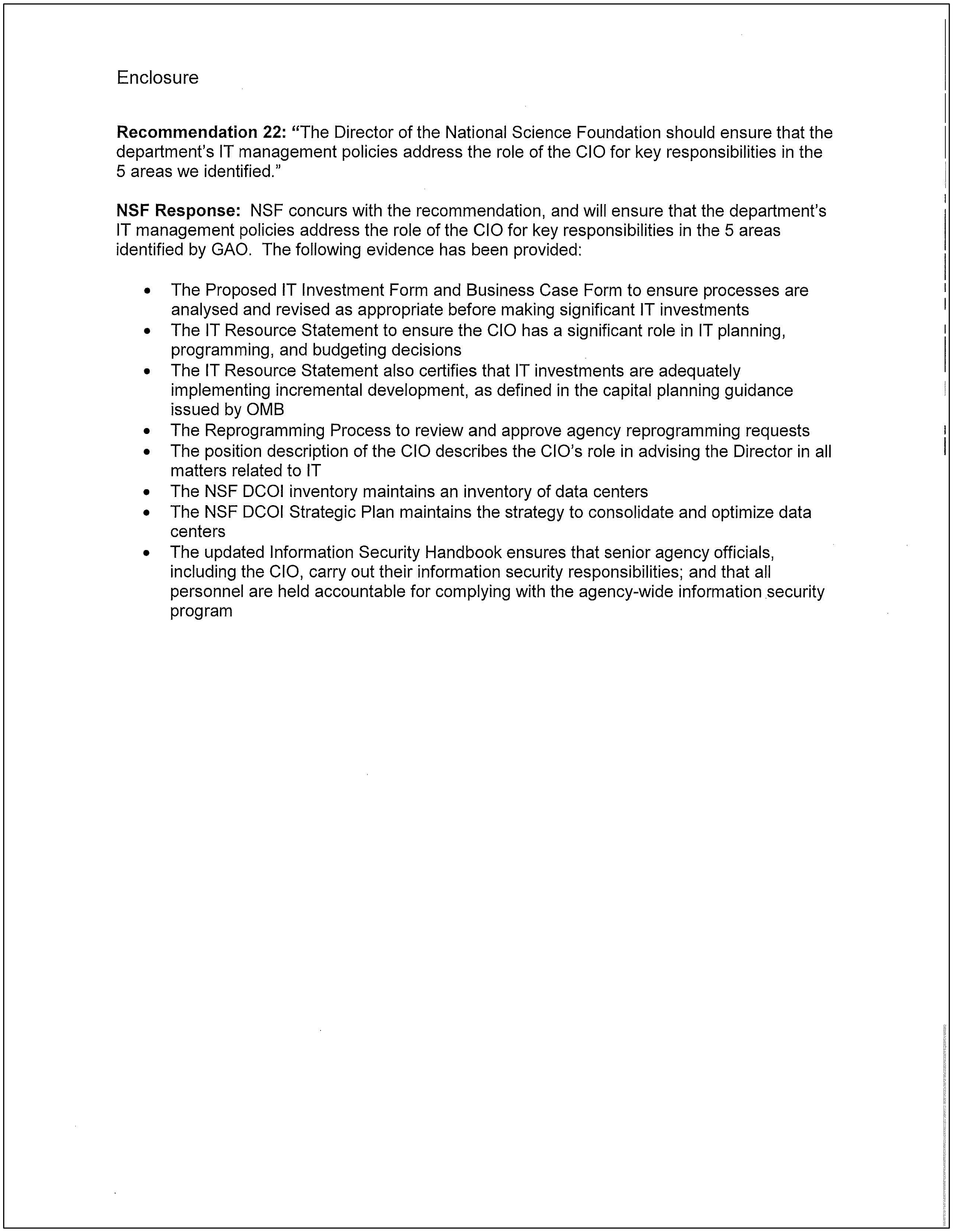
Thank you for the opportunity to review and comment on the Government and Accountability Office (GAO) draft report titled *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO 18-93).*

On behalf of the National Science Foundation (NSF), I have enclosed our comments on the draft report. NSF concurs with the recommendation and is committed to fully implementing the Federal Information Technology Acquisition Reform Act (FITARA). Since the issuance of this report, NSF has updated the agency IT security policy to provide more specificity about the role of the CIO. We have also provided GAO with documents which articulate the CIO's role in the Budgeting and IT Investment Management areas detailed in this engagement; highlighted in the enclosure.

NSF is committed to implementing appropriate improvements to ensure that the Foundation maintains sound IT management policies and appreciates GAO's work and continued interest in this area. If you have any questions, please contact Veronica Shelley, NSF Liaison to the GAO, at (703)-292-4384 or vshelley@nsf.gov.

Sincerely,

Dorothy Aronson
Chief Information Officer



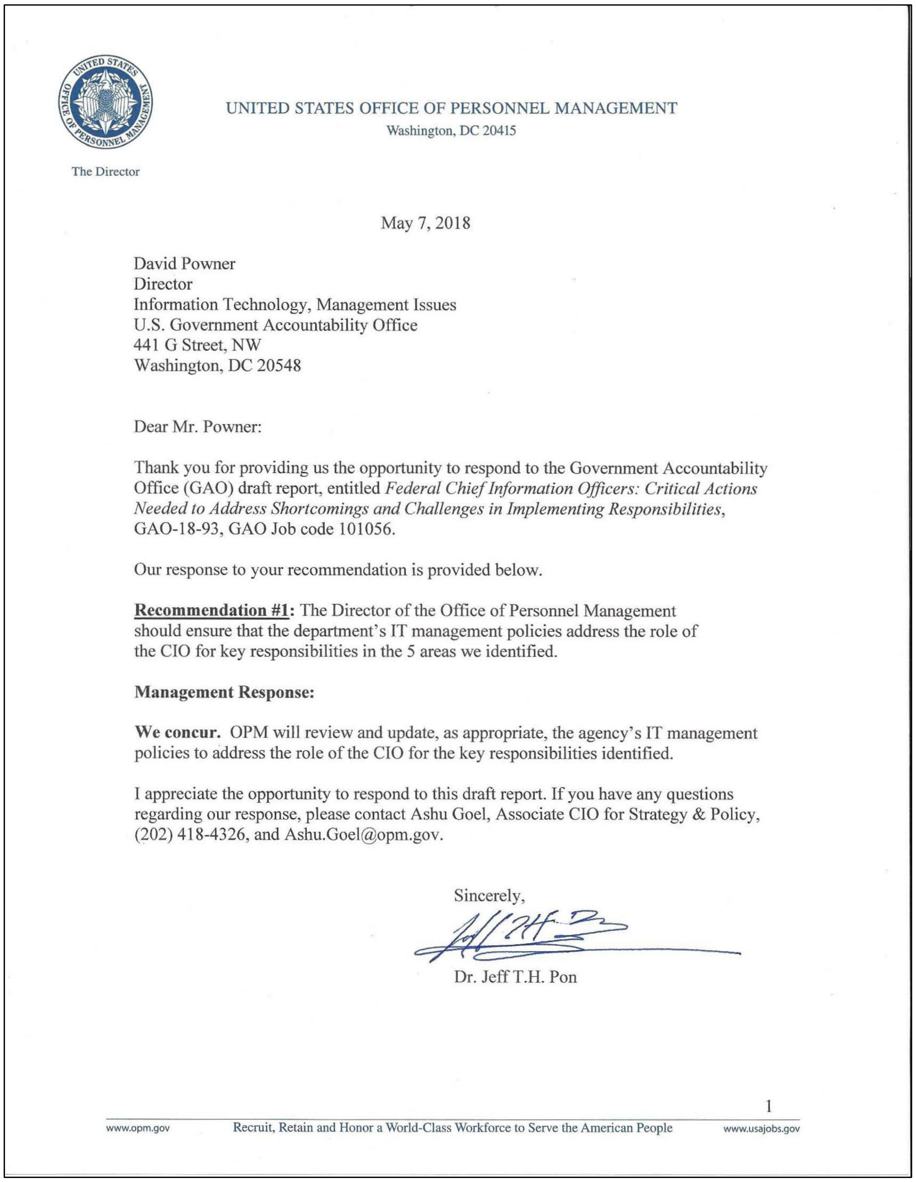
Enclosure

**Recommendation 22:** “The Director of the National Science Foundation should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified.”

**NSF Response:** NSF concurs with the recommendation, and will ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the 5 areas identified by GAO. The following evidence has been provided:

- The Proposed IT Investment Form and Business Case Form to ensure processes are analysed and revised as appropriate before making significant IT investments
- The IT Resource Statement to ensure the CIO has a significant role in IT planning, programming, and budgeting decisions
- The IT Resource Statement also certifies that IT investments are adequately implementing incremental development, as defined in the capital planning guidance issued by OMB
- The Reprogramming Process to review and approve agency reprogramming requests
- The position description of the CIO describes the CIO’s role in advising the Director in all matters related to IT
- The NSF DCOI inventory maintains an inventory of data centers
- The NSF DCOI Strategic Plan maintains the strategy to consolidate and optimize data centers
- The updated Information Security Handbook ensures that senior agency officials, including the CIO, carry out their information security responsibilities; and that all personnel are held accountable for complying with the agency-wide information security program

# Appendix XVII: Comments from the Office of Personnel Management



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

May 7, 2018

David Powner
Director
Information Technology, Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, entitled *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93, GAO Job code 101056.

Our response to your recommendation is provided below.

**Recommendation #1:** The Director of the Office of Personnel Management should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified.

**Management Response:**

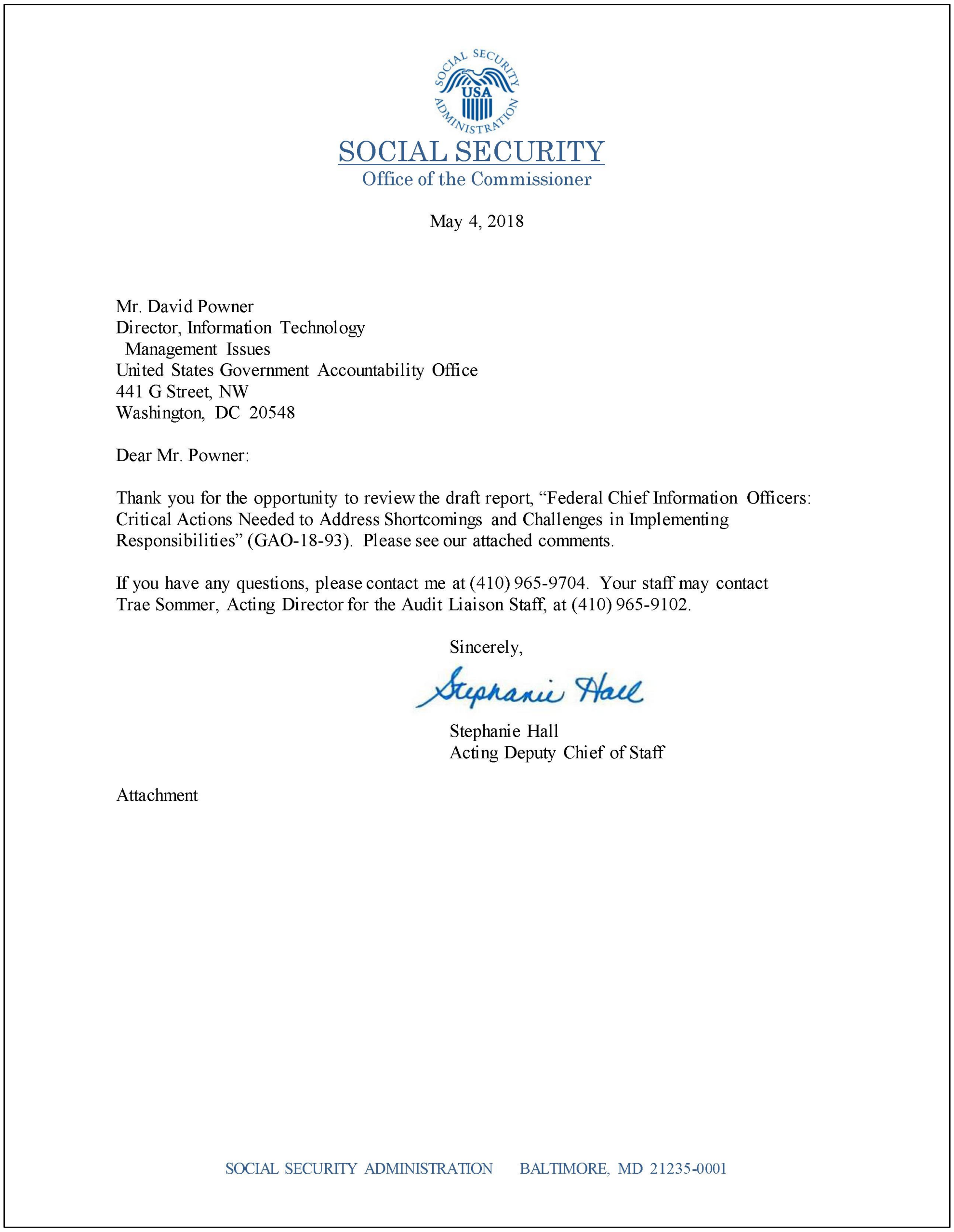
**We concur.** OPM will review and update, as appropriate, the agency's IT management policies to address the role of the CIO for the key responsibilities identified.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Ashu Goel, Associate CIO for Strategy & Policy, (202) 418-4326, and Ashu.Goel@opm.gov.

Sincerely,

Dr. Jeff T.H. Pon

# Appendix XVIII: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

May 4, 2018

Mr. David Powner
Director, Information Technology
Management Issues
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

Thank you for the opportunity to review the draft report, “Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities” (GAO-18-93). Please see our attached comments.

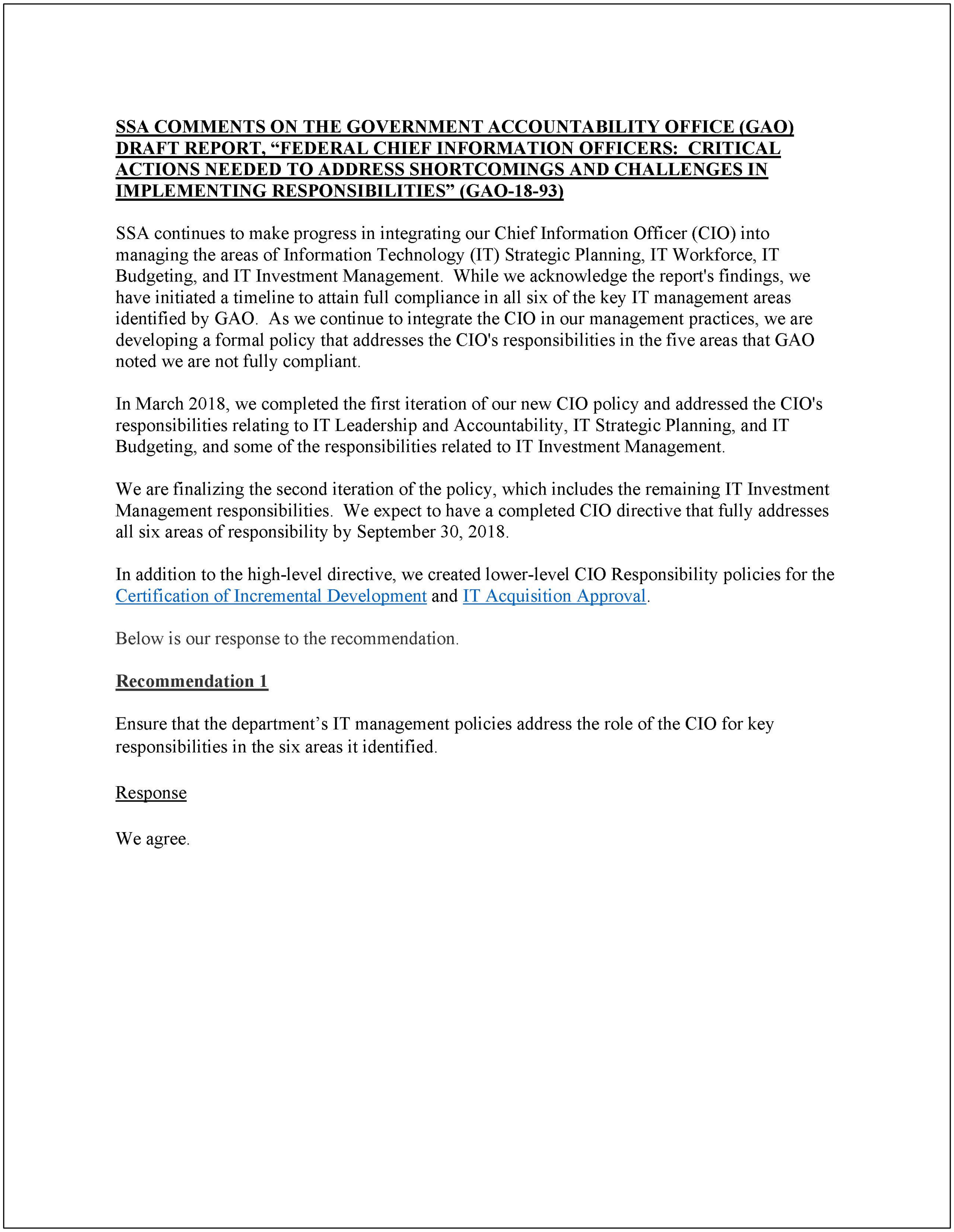
If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director for the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

Attachment



**SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES" (GAO-18-93)**

SSA continues to make progress in integrating our Chief Information Officer (CIO) into managing the areas of Information Technology (IT) Strategic Planning, IT Workforce, IT Budgeting, and IT Investment Management. While we acknowledge the report's findings, we have initiated a timeline to attain full compliance in all six of the key IT management areas identified by GAO. As we continue to integrate the CIO in our management practices, we are developing a formal policy that addresses the CIO's responsibilities in the five areas that GAO noted we are not fully compliant.

In March 2018, we completed the first iteration of our new CIO policy and addressed the CIO's responsibilities relating to IT Leadership and Accountability, IT Strategic Planning, and IT Budgeting, and some of the responsibilities related to IT Investment Management.

We are finalizing the second iteration of the policy, which includes the remaining IT Investment Management responsibilities. We expect to have a completed CIO directive that fully addresses all six areas of responsibility by September 30, 2018.

In addition to the high-level directive, we created lower-level CIO Responsibility policies for the Certification of Incremental Development and IT Acquisition Approval.

Below is our response to the recommendation.

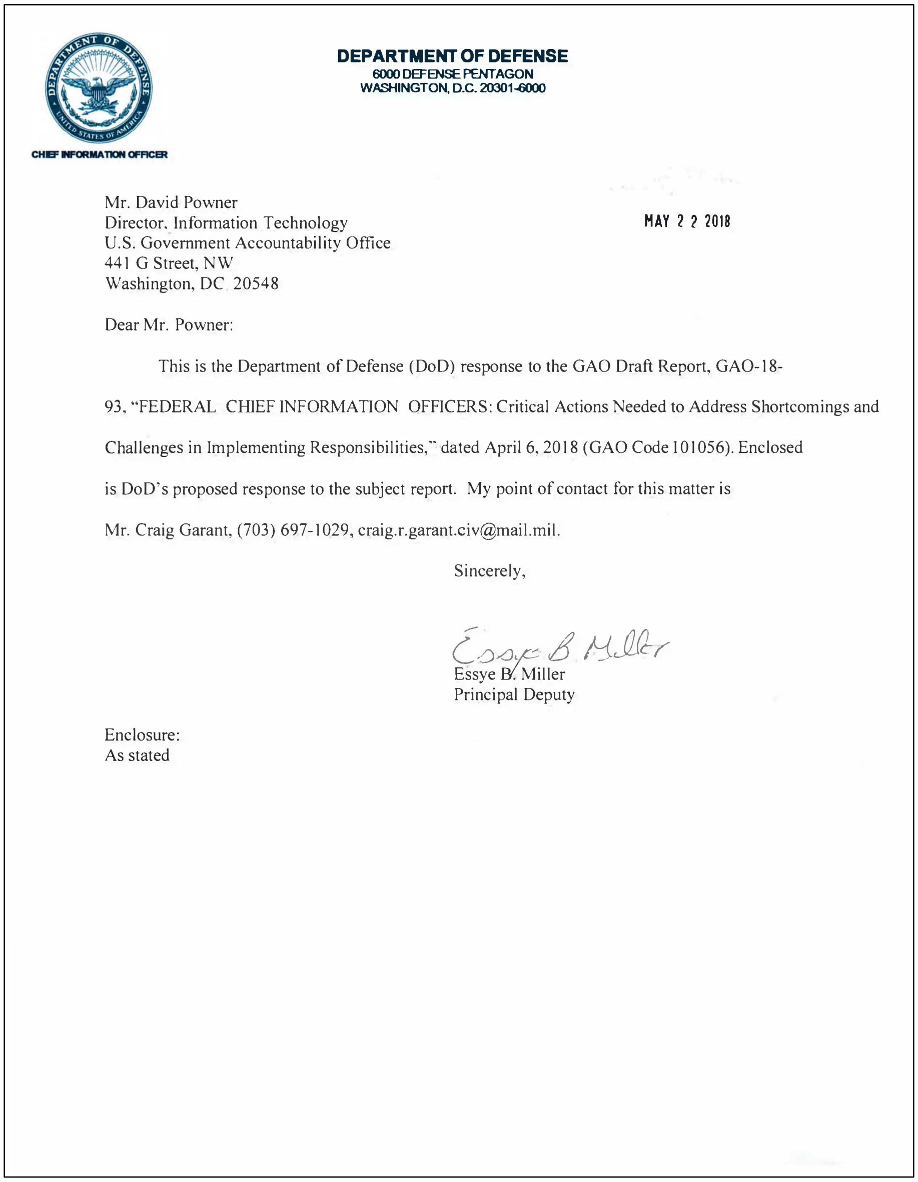
**Recommendation 1**

Ensure that the department's IT management policies address the role of the CIO for key responsibilities in the six areas it identified.

Response

We agree.

# Appendix XIX: Comments from the Department of Defense



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

CHIEF INFORMATION OFFICER

MAY 2 2 2018

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

Dear Mr. Powner:

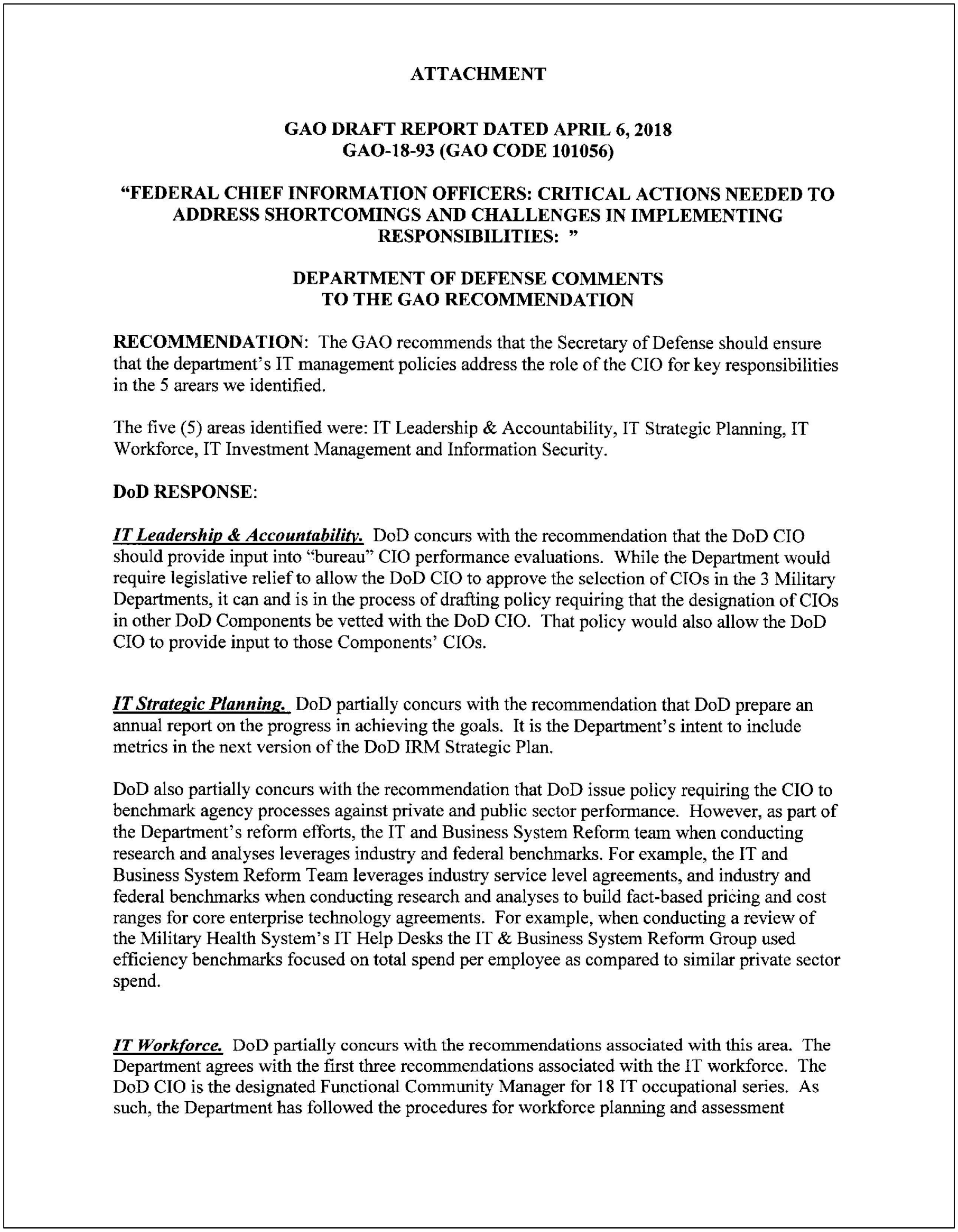
This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-18-93, "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities," dated April 6, 2018 (GAO Code 101056). Enclosed is DoD's proposed response to the subject report. My point of contact for this matter is Mr. Craig Garant, (703) 697-1029, craig.r.garant.civ@mail.mil.

Sincerely,

Essye B. Miller

Essye B. Miller
Principal Deputy

Enclosure:
As stated



ATTACHMENT

GAO DRAFT REPORT DATED APRIL 6, 2018
GAO-18-93 (GAO CODE 101056)

"FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES: "

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION

**RECOMMENDATION**: The GAO recommends that the Secretary of Defense should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 arears we identified.

The five (5) areas identified were: IT Leadership & Accountability, IT Strategic Planning, IT Workforce, IT Investment Management and Information Security.

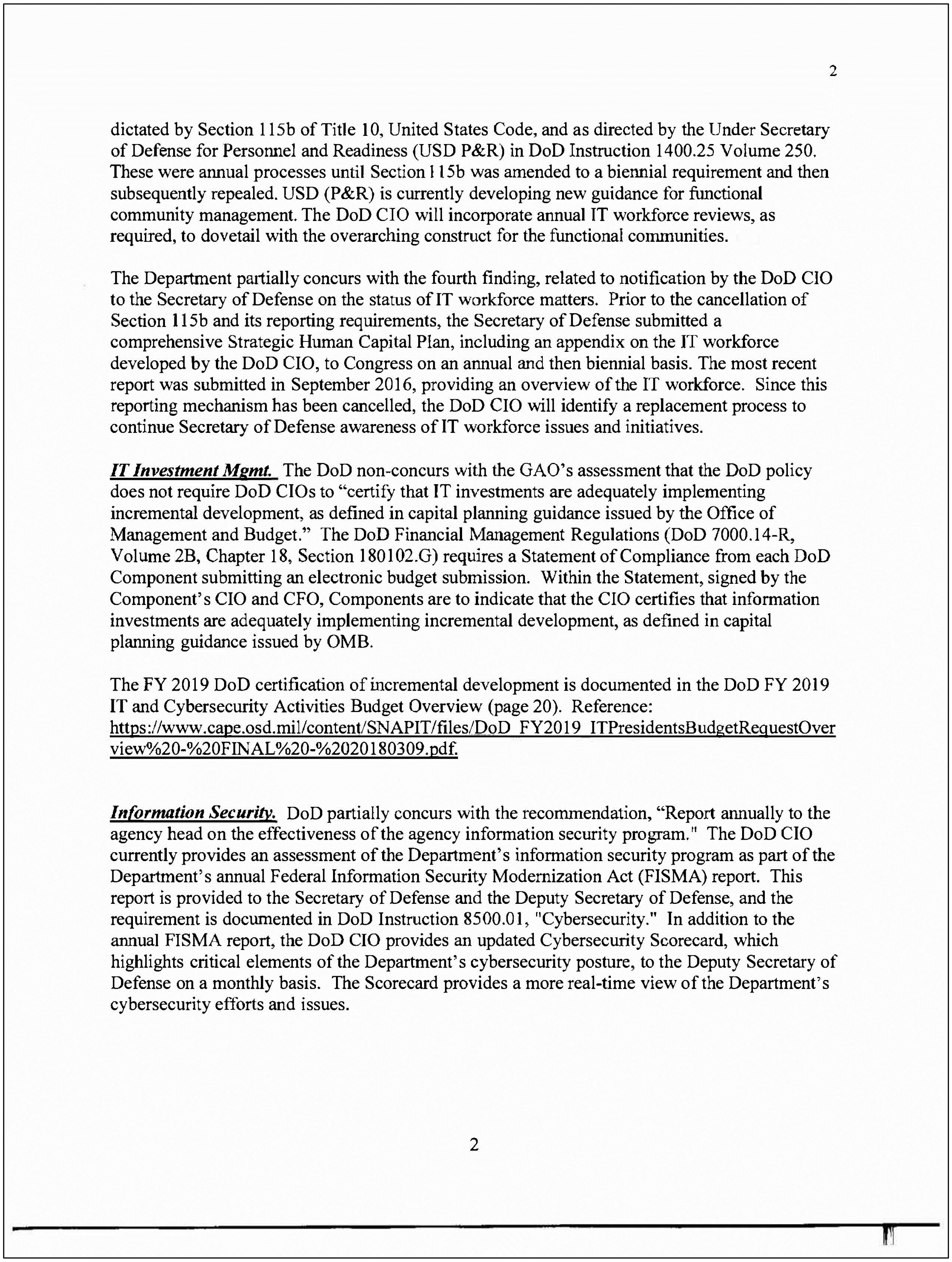
**DoD RESPONSE**:

***IT Leadership & Accountability.*** DoD concurs with the recommendation that the DoD CIO should provide input into "bureau" CIO performance evaluations. While the Department would require legislative relief to allow the DoD CIO to approve the selection of CIOs in the 3 Military Departments, it can and is in the process of drafting policy requiring that the designation of CIOs in other DoD Components be vetted with the DoD CIO. That policy would also allow the DoD CIO to provide input to those Components' CIOs.

***IT Strategic Planning.*** DoD partially concurs with the recommendation that DoD prepare an annual report on the progress in achieving the goals. It is the Department's intent to include metrics in the next version of the DoD IRM Strategic Plan.

DoD also partially concurs with the recommendation that DoD issue policy requiring the CIO to benchmark agency processes against private and public sector performance. However, as part of the Department's reform efforts, the IT and Business System Reform team when conducting research and analyses leverages industry and federal benchmarks. For example, the IT and Business System Reform Team leverages industry service level agreements, and industry and federal benchmarks when conducting research and analyses to build fact-based pricing and cost ranges for core enterprise technology agreements. For example, when conducting a review of the Military Health System's IT Help Desks the IT & Business System Reform Group used efficiency benchmarks focused on total spend per employee as compared to similar private sector spend.

***IT Workforce.*** DoD partially concurs with the recommendations associated with this area. The Department agrees with the first three recommendations associated with the IT workforce. The DoD CIO is the designated Functional Community Manager for 18 IT occupational series. As such, the Department has followed the procedures for workforce planning and assessment



dictated by Section 115b of Title 10, United States Code, and as directed by the Under Secretary of Defense for Personnel and Readiness (USD P&R) in DoD Instruction 1400.25 Volume 250. These were annual processes until Section 115b was amended to a biennial requirement and then subsequently repealed. USD (P&R) is currently developing new guidance for functional community management. The DoD CIO will incorporate annual IT workforce reviews, as required, to dovetail with the overarching construct for the functional communities.

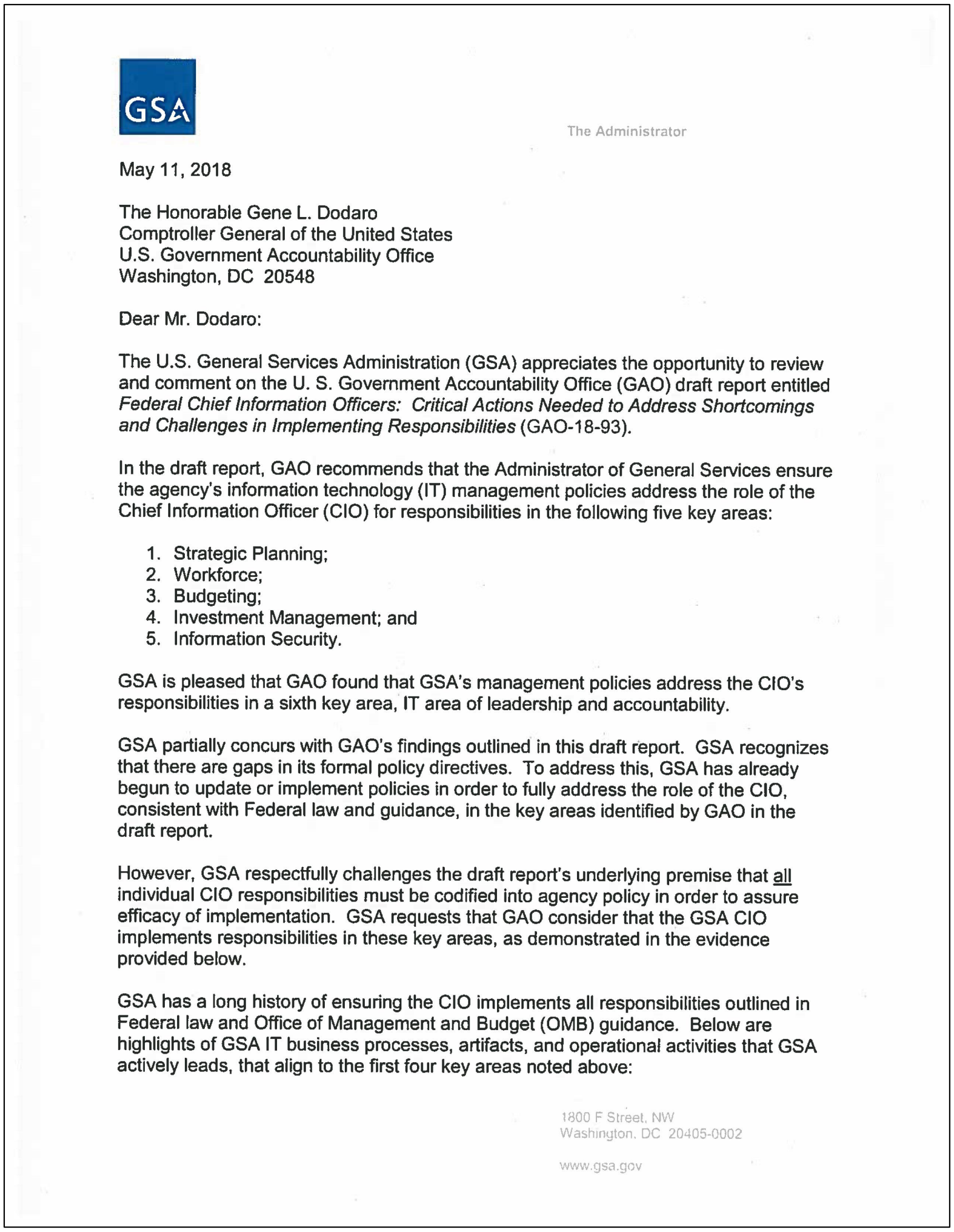
The Department partially concurs with the fourth finding, related to notification by the DoD CIO to the Secretary of Defense on the status of IT workforce matters. Prior to the cancellation of Section 115b and its reporting requirements, the Secretary of Defense submitted a comprehensive Strategic Human Capital Plan, including an appendix on the IT workforce developed by the DoD CIO, to Congress on an annual and then biennial basis. The most recent report was submitted in September 2016, providing an overview of the IT workforce. Since this reporting mechanism has been cancelled, the DoD CIO will identify a replacement process to continue Secretary of Defense awareness of IT workforce issues and initiatives.

***IT Investment Mgmt.*** The DoD non-concurs with the GAO's assessment that the DoD policy does not require DoD CIOs to "certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget." The DoD Financial Management Regulations (DoD 7000.14-R, Volume 2B, Chapter 18, Section 180102.G) requires a Statement of Compliance from each DoD Component submitting an electronic budget submission. Within the Statement, signed by the Component's CIO and CFO, Components are to indicate that the CIO certifies that information investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB.

The FY 2019 DoD certification of incremental development is documented in the DoD FY 2019 IT and Cybersecurity Activities Budget Overview (page 20). Reference: https://www.cape.osd.mil/content/SNAPIT/files/DoD_FY2019_ITPresidentsBudgetRequestOverview%20-%20FINAL%20-%2020180309.pdf.

***Information Security.*** DoD partially concurs with the recommendation, "Report annually to the agency head on the effectiveness of the agency information security program." The DoD CIO currently provides an assessment of the Department's information security program as part of the Department's annual Federal Information Security Modernization Act (FISMA) report. This report is provided to the Secretary of Defense and the Deputy Secretary of Defense, and the requirement is documented in DoD Instruction 8500.01, "Cybersecurity." In addition to the annual FISMA report, the DoD CIO provides an updated Cybersecurity Scorecard, which highlights critical elements of the Department's cybersecurity posture, to the Deputy Secretary of Defense on a monthly basis. The Scorecard provides a more real-time view of the Department's cybersecurity efforts and issues.

# Appendix XX: Comments from the General Services Administration



GSA

The Administrator

May 11, 2018

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U. S. Government Accountability Office (GAO) draft report entitled *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* (GAO-18-93).

In the draft report, GAO recommends that the Administrator of General Services ensure the agency's information technology (IT) management policies address the role of the Chief Information Officer (CIO) for responsibilities in the following five key areas:

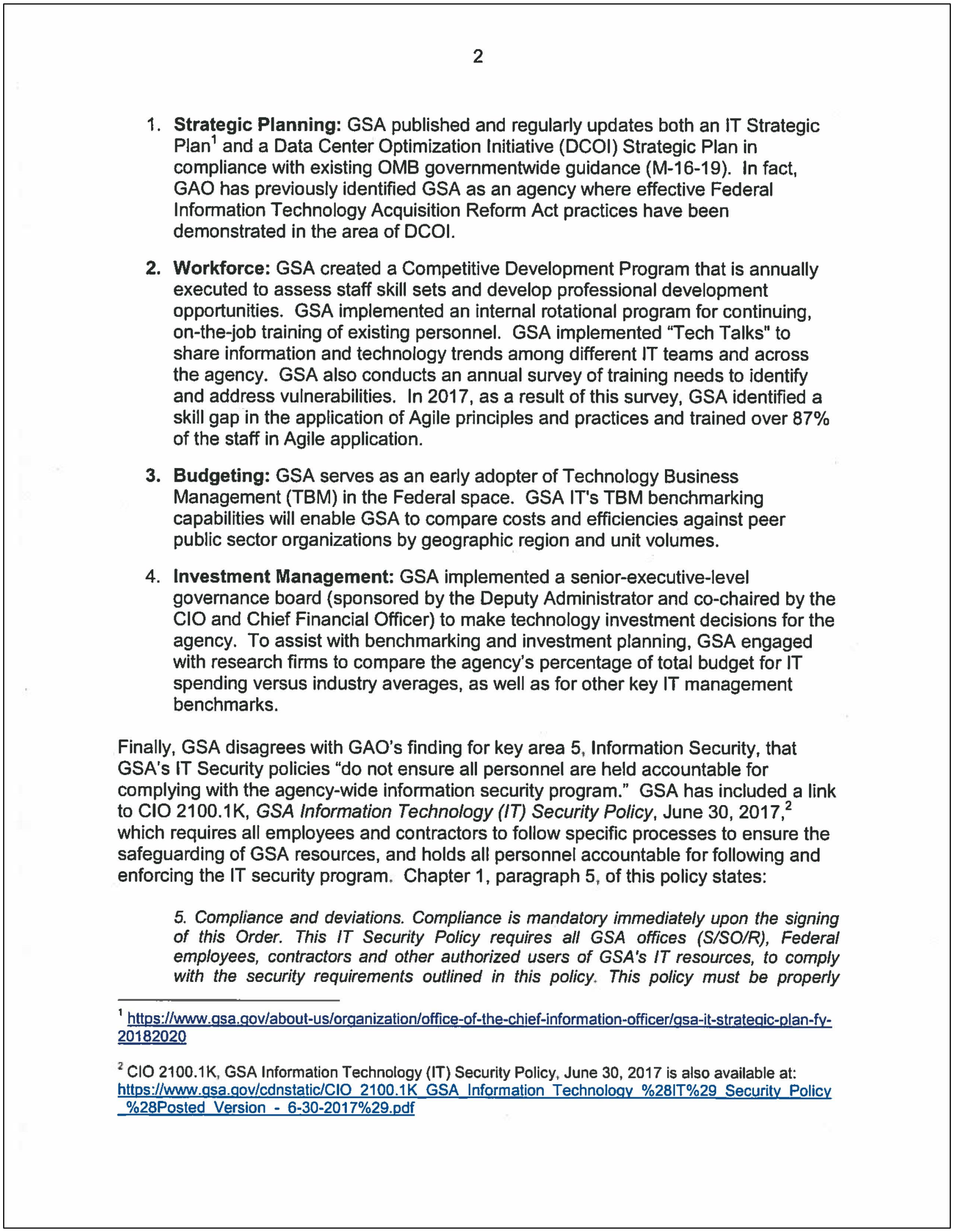
1. Strategic Planning;
2. Workforce;
3. Budgeting;
4. Investment Management; and
5. Information Security.

GSA is pleased that GAO found that GSA's management policies address the CIO's responsibilities in a sixth key area, IT area of leadership and accountability.

GSA partially concurs with GAO's findings outlined in this draft report. GSA recognizes that there are gaps in its formal policy directives. To address this, GSA has already begun to update or implement policies in order to fully address the role of the CIO, consistent with Federal law and guidance, in the key areas identified by GAO in the draft report.

However, GSA respectfully challenges the draft report's underlying premise that all individual CIO responsibilities must be codified into agency policy in order to assure efficacy of implementation. GSA requests that GAO consider that the GSA CIO implements responsibilities in these key areas, as demonstrated in the evidence provided below.

GSA has a long history of ensuring the CIO implements all responsibilities outlined in Federal law and Office of Management and Budget (OMB) guidance. Below are highlights of GSA IT business processes, artifacts, and operational activities that GSA actively leads, that align to the first four key areas noted above:



1. **Strategic Planning:** GSA published and regularly updates both an IT Strategic Plan[1] and a Data Center Optimization Initiative (DCOI) Strategic Plan in compliance with existing OMB governmentwide guidance (M-16-19). In fact, GAO has previously identified GSA as an agency where effective Federal Information Technology Acquisition Reform Act practices have been demonstrated in the area of DCOI.

2. **Workforce:** GSA created a Competitive Development Program that is annually executed to assess staff skill sets and develop professional development opportunities. GSA implemented an internal rotational program for continuing, on-the-job training of existing personnel. GSA implemented "Tech Talks" to share information and technology trends among different IT teams and across the agency. GSA also conducts an annual survey of training needs to identify and address vulnerabilities. In 2017, as a result of this survey, GSA identified a skill gap in the application of Agile principles and practices and trained over 87% of the staff in Agile application.

3. **Budgeting:** GSA serves as an early adopter of Technology Business Management (TBM) in the Federal space. GSA IT's TBM benchmarking capabilities will enable GSA to compare costs and efficiencies against peer public sector organizations by geographic region and unit volumes.

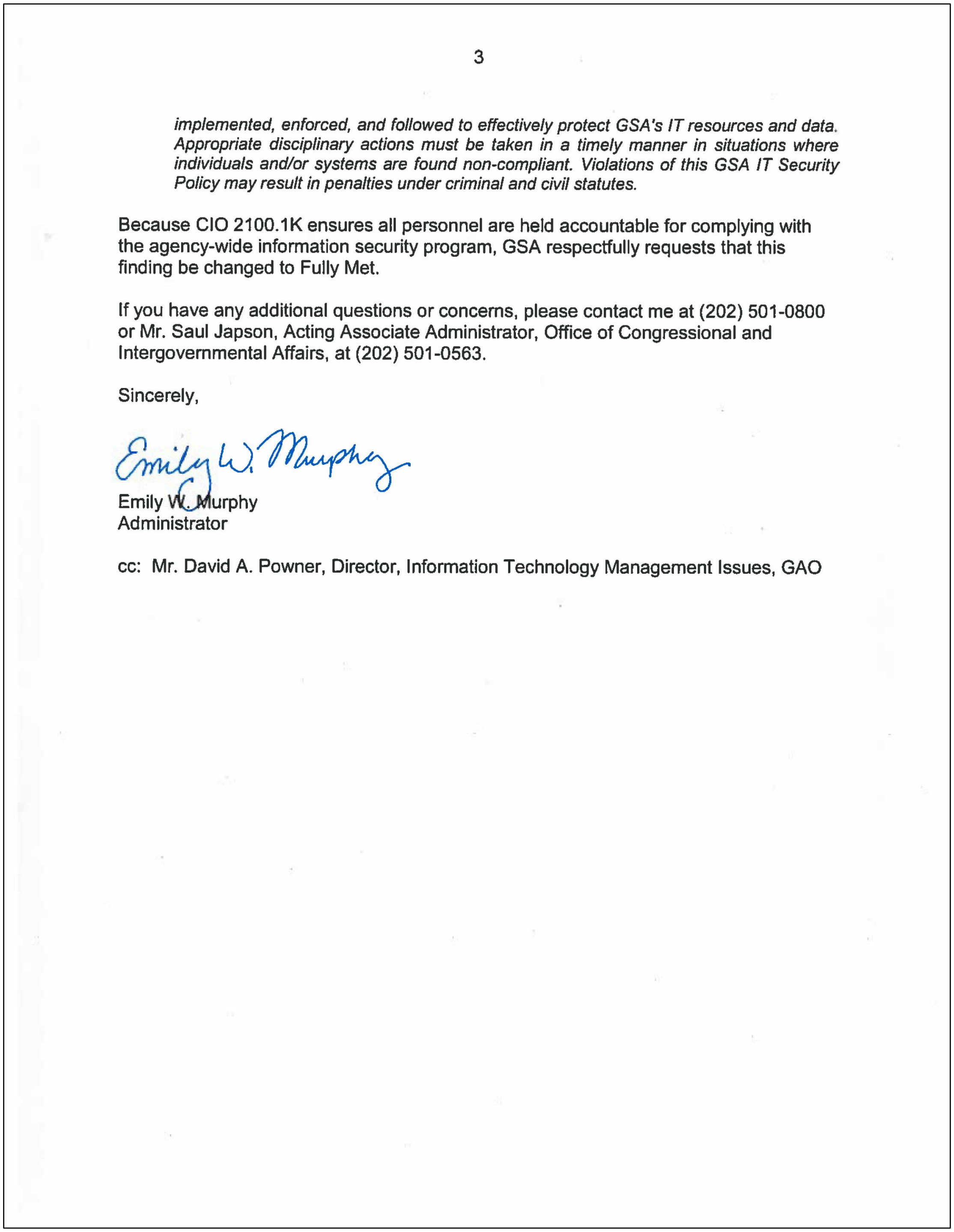
4. **Investment Management:** GSA implemented a senior-executive-level governance board (sponsored by the Deputy Administrator and co-chaired by the CIO and Chief Financial Officer) to make technology investment decisions for the agency. To assist with benchmarking and investment planning, GSA engaged with research firms to compare the agency's percentage of total budget for IT spending versus industry averages, as well as for other key IT management benchmarks.

Finally, GSA disagrees with GAO's finding for key area 5, Information Security, that GSA's IT Security policies "do not ensure all personnel are held accountable for complying with the agency-wide information security program." GSA has included a link to CIO 2100.1K, *GSA Information Technology (IT) Security Policy*, June 30, 2017,[2] which requires all employees and contractors to follow specific processes to ensure the safeguarding of GSA resources, and holds all personnel accountable for following and enforcing the IT security program. Chapter 1, paragraph 5, of this policy states:

> *5. Compliance and deviations. Compliance is mandatory immediately upon the signing of this Order. This IT Security Policy requires all GSA offices (S/SO/R), Federal employees, contractors and other authorized users of GSA's IT resources, to comply with the security requirements outlined in this policy. This policy must be properly*

[1] https://www.gsa.gov/about-us/organization/office-of-the-chief-information-officer/gsa-it-strategic-plan-fy-20182020

[2] CIO 2100.1K, GSA Information Technology (IT) Security Policy, June 30, 2017 is also available at: https://www.gsa.gov/cdnstatic/CIO_2100.1K_GSA_Information_Technology_%28IT%29_Security_Policy_%28Posted_Version_-_6-30-2017%29.pdf



> *implemented, enforced, and followed to effectively protect GSA's IT resources and data. Appropriate disciplinary actions must be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of this GSA IT Security Policy may result in penalties under criminal and civil statutes.*

Because CIO 2100.1K ensures all personnel are held accountable for complying with the agency-wide information security program, GSA respectfully requests that this finding be changed to Fully Met.

If you have any additional questions or concerns, please contact me at (202) 501-0800 or Mr. Saul Japson, Acting Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

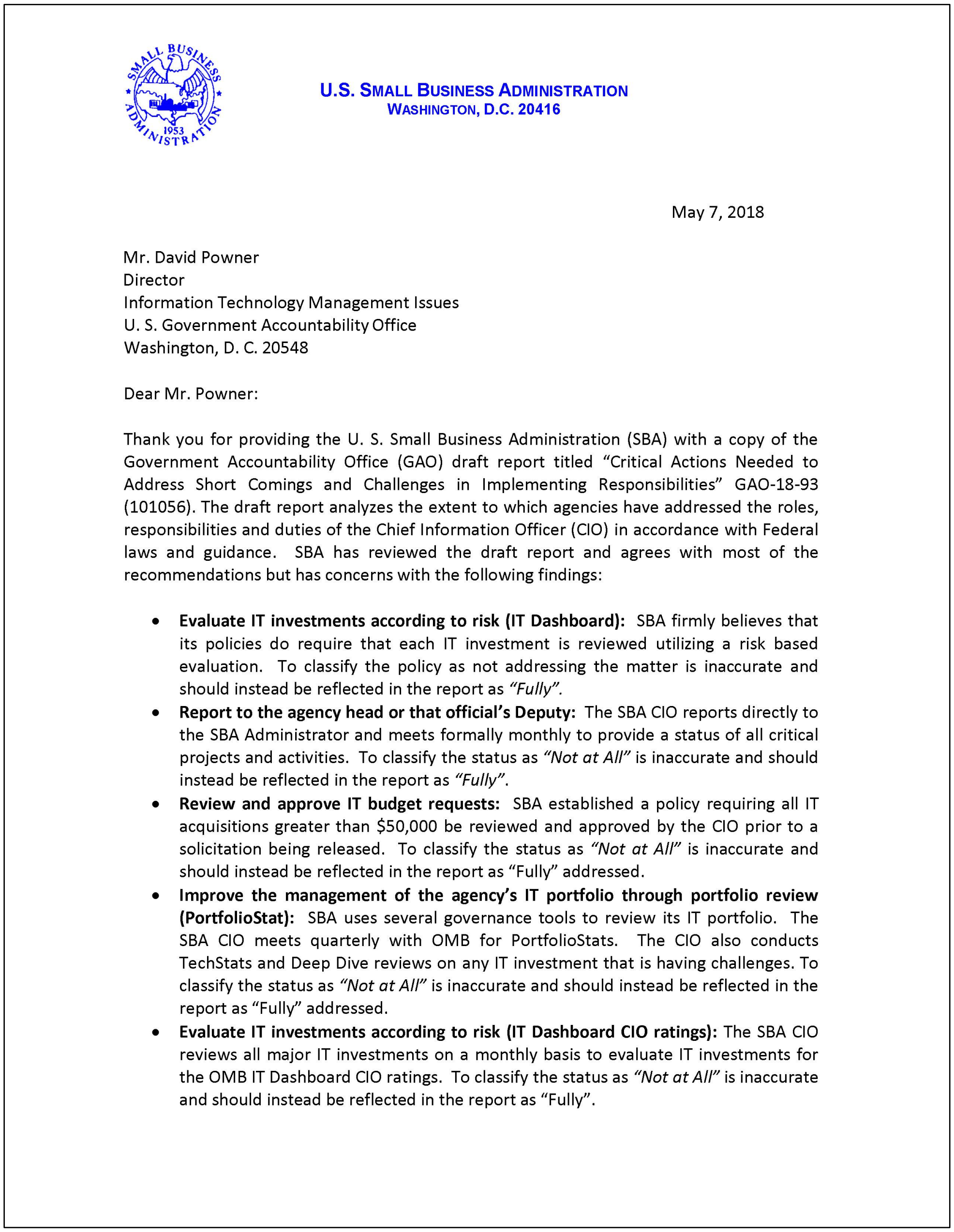
Sincerely,

Emily W. Murphy

Emily W. Murphy<br>
Administrator

cc: Mr. David A. Powner, Director, Information Technology Management Issues, GAO

# Appendix XXI: Comments from the Small Business Administration



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

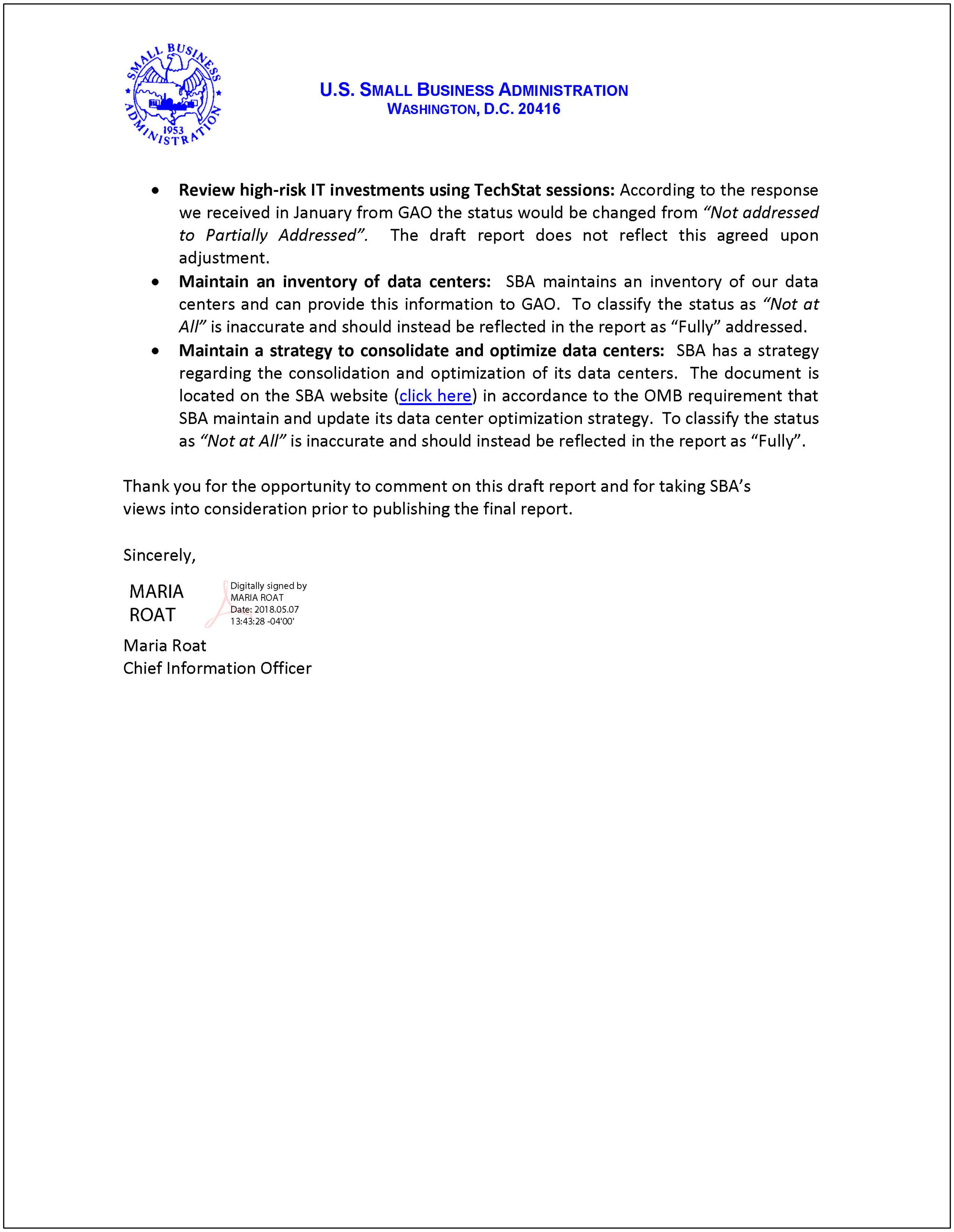
May 7, 2018

Mr. David Powner
Director
Information Technology Management Issues
U. S. Government Accountability Office
Washington, D. C. 20548

Dear Mr. Powner:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled "Critical Actions Needed to Address Short Comings and Challenges in Implementing Responsibilities" GAO-18-93 (101056). The draft report analyzes the extent to which agencies have addressed the roles, responsibilities and duties of the Chief Information Officer (CIO) in accordance with Federal laws and guidance. SBA has reviewed the draft report and agrees with most of the recommendations but has concerns with the following findings:

- **Evaluate IT investments according to risk (IT Dashboard):** SBA firmly believes that its policies do require that each IT investment is reviewed utilizing a risk based evaluation. To classify the policy as not addressing the matter is inaccurate and should instead be reflected in the report as *"Fully"*.
- **Report to the agency head or that official's Deputy:** The SBA CIO reports directly to the SBA Administrator and meets formally monthly to provide a status of all critical projects and activities. To classify the status as *"Not at All"* is inaccurate and should instead be reflected in the report as *"Fully"*.
- **Review and approve IT budget requests:** SBA established a policy requiring all IT acquisitions greater than $50,000 be reviewed and approved by the CIO prior to a solicitation being released. To classify the status as *"Not at All"* is inaccurate and should instead be reflected in the report as "Fully" addressed.
- **Improve the management of the agency's IT portfolio through portfolio review (PortfolioStat):** SBA uses several governance tools to review its IT portfolio. The SBA CIO meets quarterly with OMB for PortfolioStats. The CIO also conducts TechStats and Deep Dive reviews on any IT investment that is having challenges. To classify the status as *"Not at All"* is inaccurate and should instead be reflected in the report as "Fully" addressed.
- **Evaluate IT investments according to risk (IT Dashboard CIO ratings):** The SBA CIO reviews all major IT investments on a monthly basis to evaluate IT investments for the OMB IT Dashboard CIO ratings. To classify the status as *"Not at All"* is inaccurate and should instead be reflected in the report as "Fully".



- **Review high-risk IT investments using TechStat sessions:** According to the response we received in January from GAO the status would be changed from *"Not addressed to Partially Addressed".* The draft report does not reflect this agreed upon adjustment.
- **Maintain an inventory of data centers:** SBA maintains an inventory of our data centers and can provide this information to GAO. To classify the status as *"Not at All"* is inaccurate and should instead be reflected in the report as "Fully" addressed.
- **Maintain a strategy to consolidate and optimize data centers:** SBA has a strategy regarding the consolidation and optimization of its data centers. The document is located on the SBA website (click here) in accordance to the OMB requirement that SBA maintain and update its data center optimization strategy. To classify the status as *"Not at All"* is inaccurate and should instead be reflected in the report as "Fully".

Thank you for the opportunity to comment on this draft report and for taking SBA's views into consideration prior to publishing the final report.

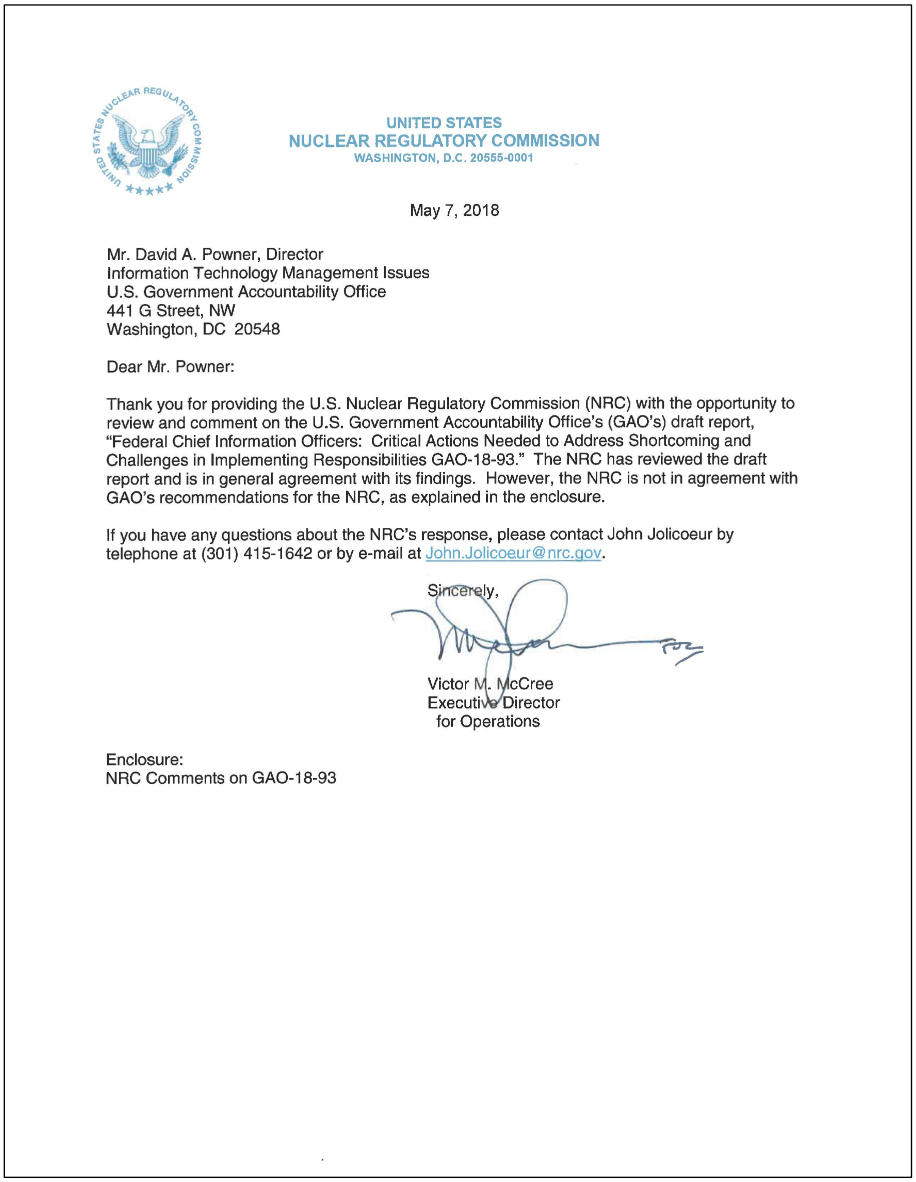
Sincerely,

MARIA
ROAT

Digitally signed by
MARIA ROAT
Date: 2018.05.07
13:43:28 -04'00'

Maria Roat
Chief Information Officer

# Appendix XXII: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

May 7, 2018

Mr. David A. Powner, Director
Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Powner:

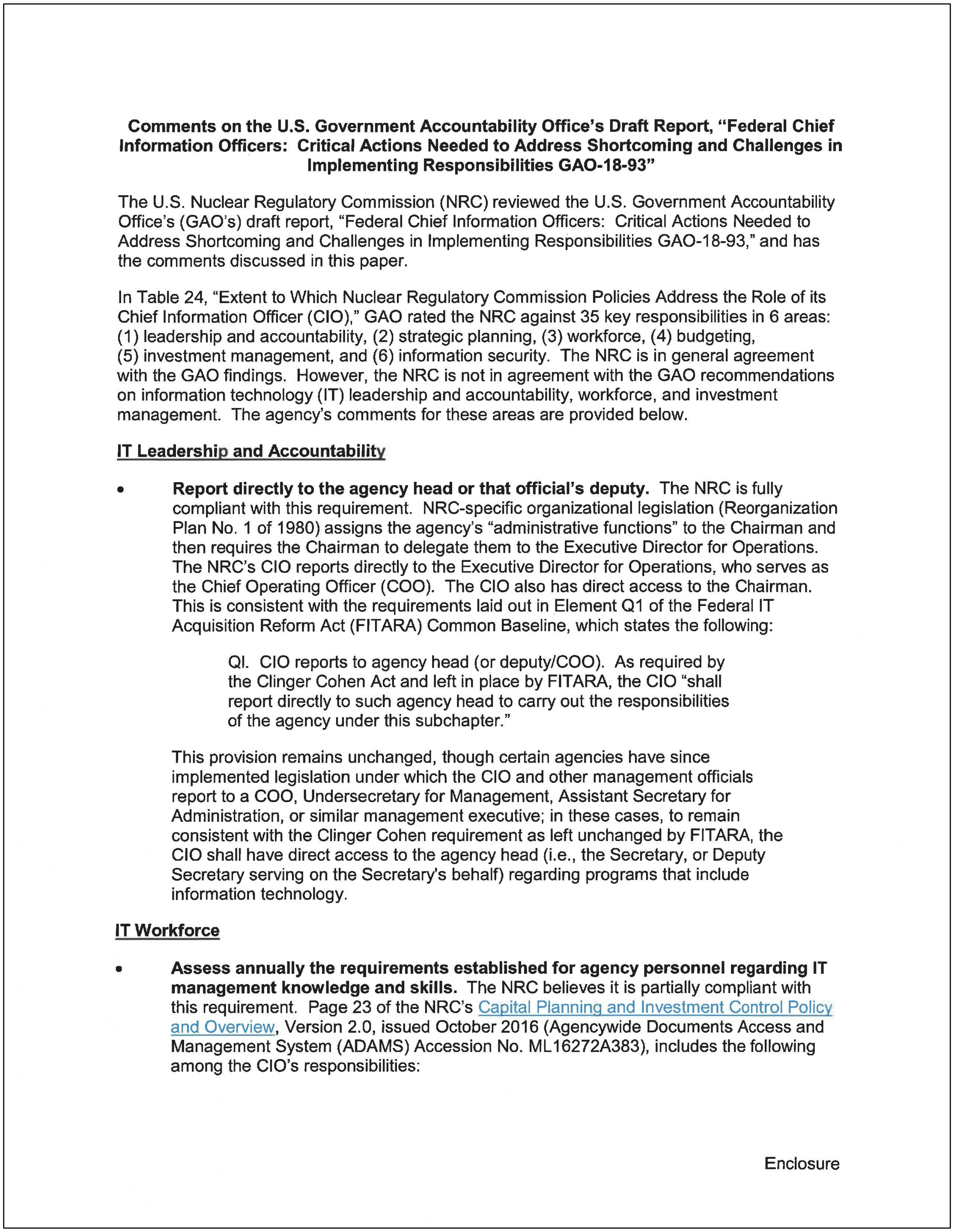
Thank you for providing the U.S. Nuclear Regulatory Commission (NRC) with the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93." The NRC has reviewed the draft report and is in general agreement with its findings. However, the NRC is not in agreement with GAO's recommendations for the NRC, as explained in the enclosure.

If you have any questions about the NRC's response, please contact John Jolicoeur by telephone at (301) 415-1642 or by e-mail at John.Jolicoeur@nrc.gov.

Sincerely,

Victor M. McCree
Executive Director
for Operations

Enclosure:
NRC Comments on GAO-18-93



**Comments on the U.S. Government Accountability Office's Draft Report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93"**

The U.S. Nuclear Regulatory Commission (NRC) reviewed the U.S. Government Accountability Office's (GAO's) draft report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93," and has the comments discussed in this paper.

In Table 24, "Extent to Which Nuclear Regulatory Commission Policies Address the Role of its Chief Information Officer (CIO)," GAO rated the NRC against 35 key responsibilities in 6 areas: (1) leadership and accountability, (2) strategic planning, (3) workforce, (4) budgeting, (5) investment management, and (6) information security. The NRC is in general agreement with the GAO findings. However, the NRC is not in agreement with the GAO recommendations on information technology (IT) leadership and accountability, workforce, and investment management. The agency's comments for these areas are provided below.

**IT Leadership and Accountability**

- **Report directly to the agency head or that official's deputy.** The NRC is fully compliant with this requirement. NRC-specific organizational legislation (Reorganization Plan No. 1 of 1980) assigns the agency's "administrative functions" to the Chairman and then requires the Chairman to delegate them to the Executive Director for Operations. The NRC's CIO reports directly to the Executive Director for Operations, who serves as the Chief Operating Officer (COO). The CIO also has direct access to the Chairman. This is consistent with the requirements laid out in Element Q1 of the Federal IT Acquisition Reform Act (FITARA) Common Baseline, which states the following:

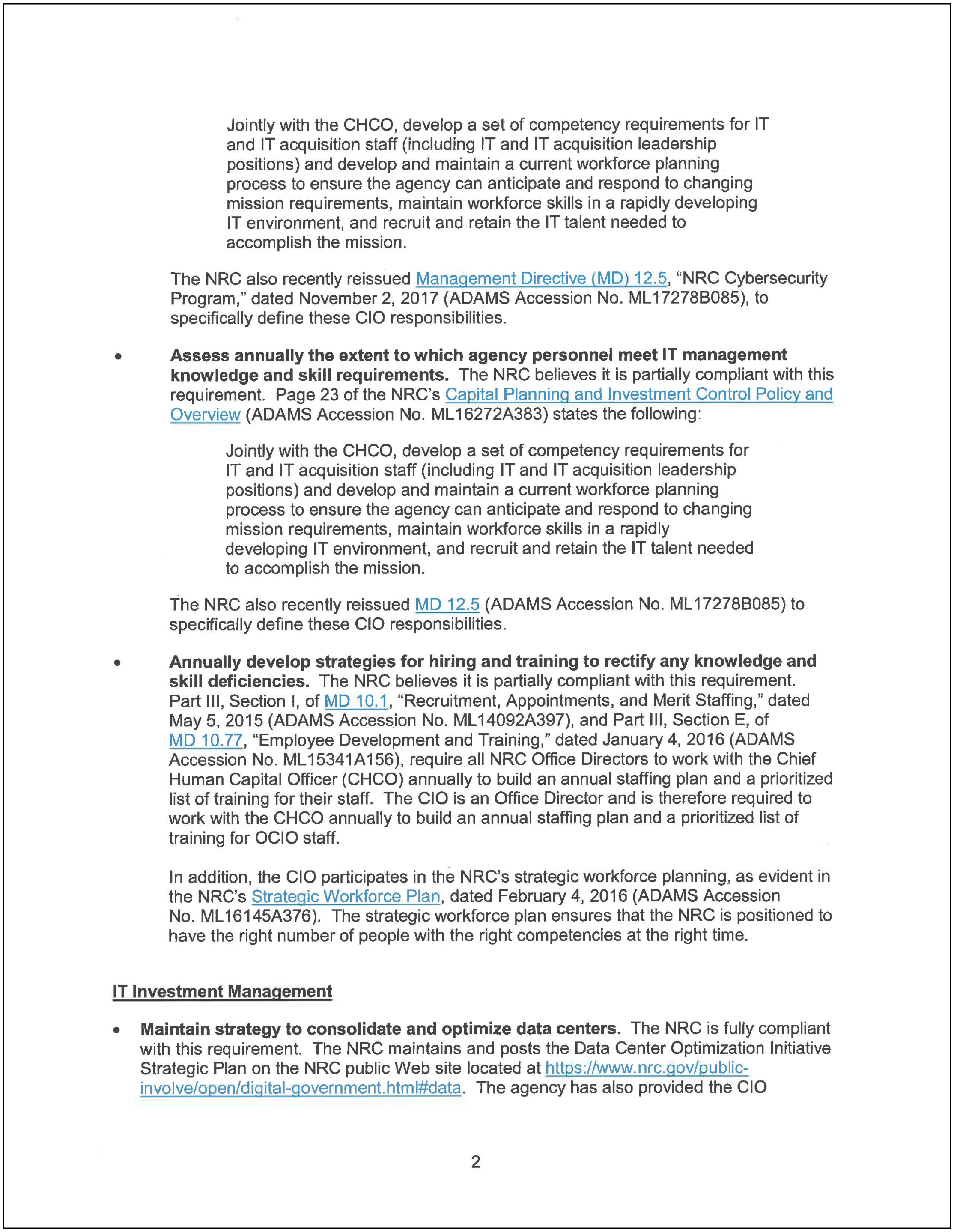
  > QI. CIO reports to agency head (or deputy/COO). As required by the Clinger Cohen Act and left in place by FITARA, the CIO "shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter."

  This provision remains unchanged, though certain agencies have since implemented legislation under which the CIO and other management officials report to a COO, Undersecretary for Management, Assistant Secretary for Administration, or similar management executive; in these cases, to remain consistent with the Clinger Cohen requirement as left unchanged by FITARA, the CIO shall have direct access to the agency head (i.e., the Secretary, or Deputy Secretary serving on the Secretary's behalf) regarding programs that include information technology.

**IT Workforce**

- **Assess annually the requirements established for agency personnel regarding IT management knowledge and skills.** The NRC believes it is partially compliant with this requirement. Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview, Version 2.0, issued October 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16272A383), includes the following among the CIO's responsibilities:

Enclosure



> Jointly with the CHCO, develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership positions) and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

The NRC also recently reissued Management Directive (MD) 12.5, "NRC Cybersecurity Program," dated November 2, 2017 (ADAMS Accession No. ML17278B085), to specifically define these CIO responsibilities.

- **Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements.** The NRC believes it is partially compliant with this requirement. Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML16272A383) states the following:

  > Jointly with the CHCO, develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership positions) and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

  The NRC also recently reissued MD 12.5 (ADAMS Accession No. ML17278B085) to specifically define these CIO responsibilities.

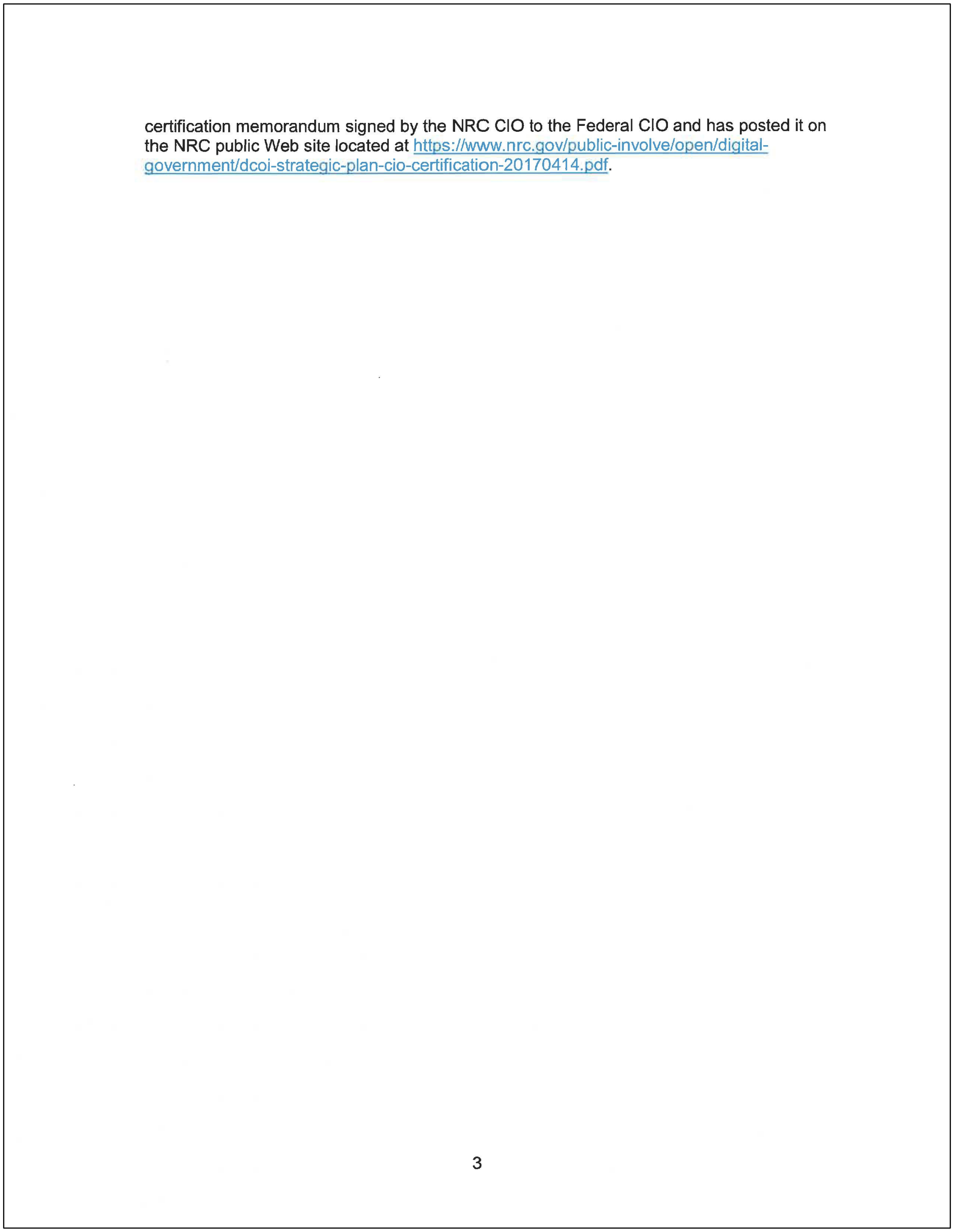
- **Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies.** The NRC believes it is partially compliant with this requirement. Part III, Section I, of MD 10.1, "Recruitment, Appointments, and Merit Staffing," dated May 5, 2015 (ADAMS Accession No. ML14092A397), and Part III, Section E, of MD 10.77, "Employee Development and Training," dated January 4, 2016 (ADAMS Accession No. ML15341A156), require all NRC Office Directors to work with the Chief Human Capital Officer (CHCO) annually to build an annual staffing plan and a prioritized list of training for their staff. The CIO is an Office Director and is therefore required to work with the CHCO annually to build an annual staffing plan and a prioritized list of training for OCIO staff.

  In addition, the CIO participates in the NRC's strategic workforce planning, as evident in the NRC's Strategic Workforce Plan, dated February 4, 2016 (ADAMS Accession No. ML16145A376). The strategic workforce plan ensures that the NRC is positioned to have the right number of people with the right competencies at the right time.

<u>IT Investment Management</u>

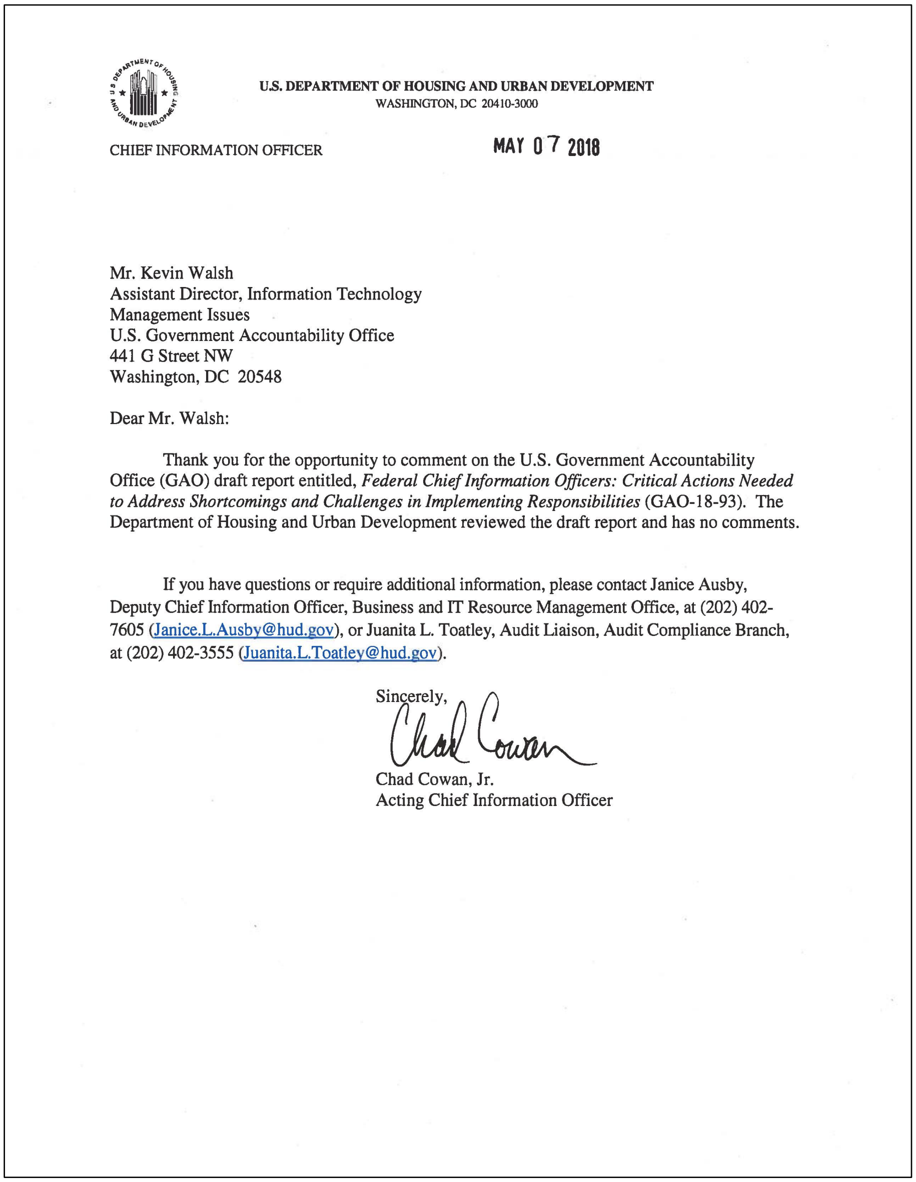
- **Maintain strategy to consolidate and optimize data centers.** The NRC is fully compliant with this requirement. The NRC maintains and posts the Data Center Optimization Initiative Strategic Plan on the NRC public Web site located at https://www.nrc.gov/public-involve/open/digital-government.html#data. The agency has also provided the CIO

2



certification memorandum signed by the NRC CIO to the Federal CIO and has posted it on the NRC public Web site located at https://www.nrc.gov/public-involve/open/digital-government/dcoi-strategic-plan-cio-certification-20170414.pdf.

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



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

CHIEF INFORMATION OFFICER

MAY 07 2018

Mr. Kevin Walsh
Assistant Director, Information Technology
Management Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Walsh:

Thank you for the opportunity to comment on the U.S. Government Accountability Office (GAO) draft report entitled, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* (GAO-18-93). The Department of Housing and Urban Development reviewed the draft report and has no comments.

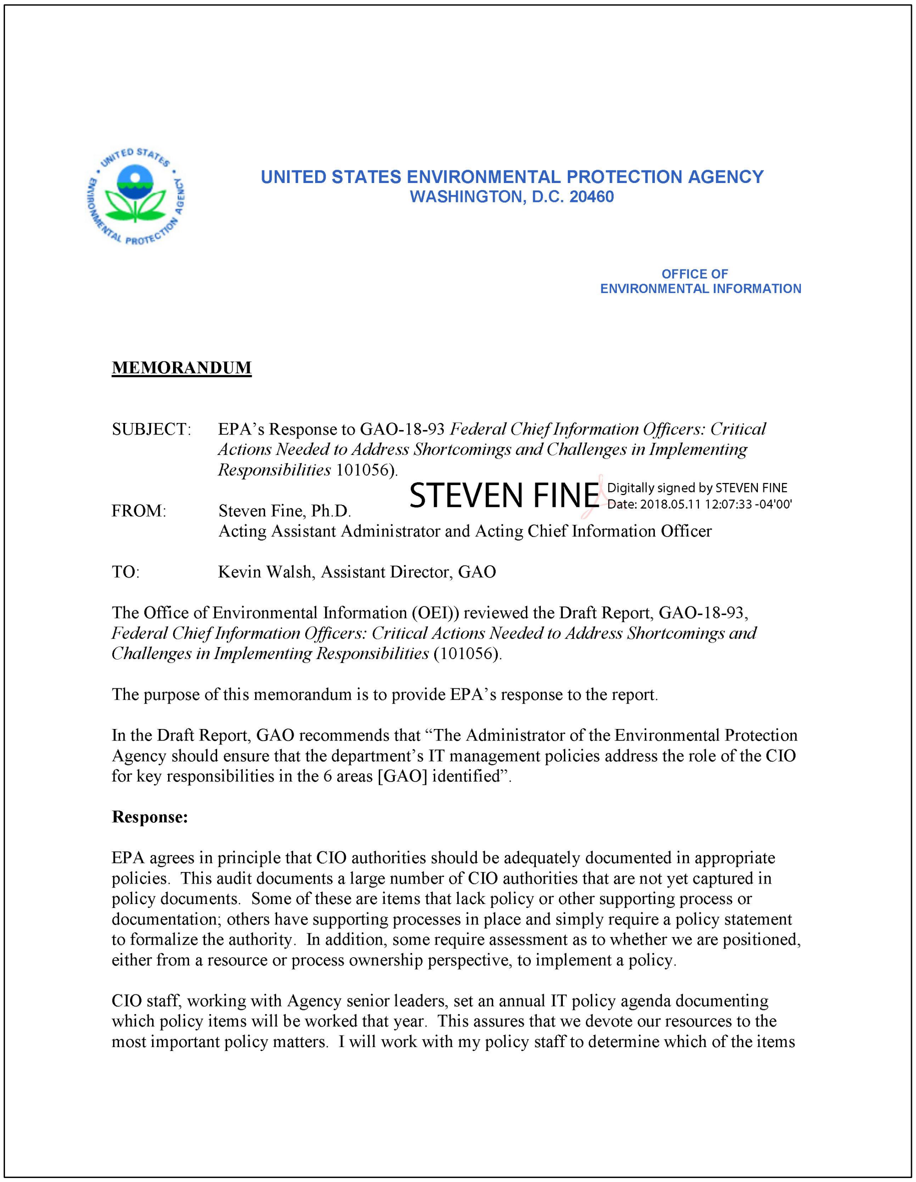
If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 (Janice.L.Ausby@hud.gov), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.gov).

Sincerely,

Chad Cowan

Chad Cowan, Jr.
Acting Chief Information Officer

# Appendix XXIV: Comments from the Environmental Protection Agency



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

OFFICE OF
ENVIRONMENTAL INFORMATION

**MEMORANDUM**

SUBJECT: EPA's Response to GAO-18-93 *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* 101056).

FROM: Steven Fine, Ph.D. STEVEN FINE Digitally signed by STEVEN FINE Date: 2018.05.11 12:07:33 -04'00'
Acting Assistant Administrator and Acting Chief Information Officer

TO: Kevin Walsh, Assistant Director, GAO

The Office of Environmental Information (OEI)) reviewed the Draft Report, GAO-18-93, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities* (101056).

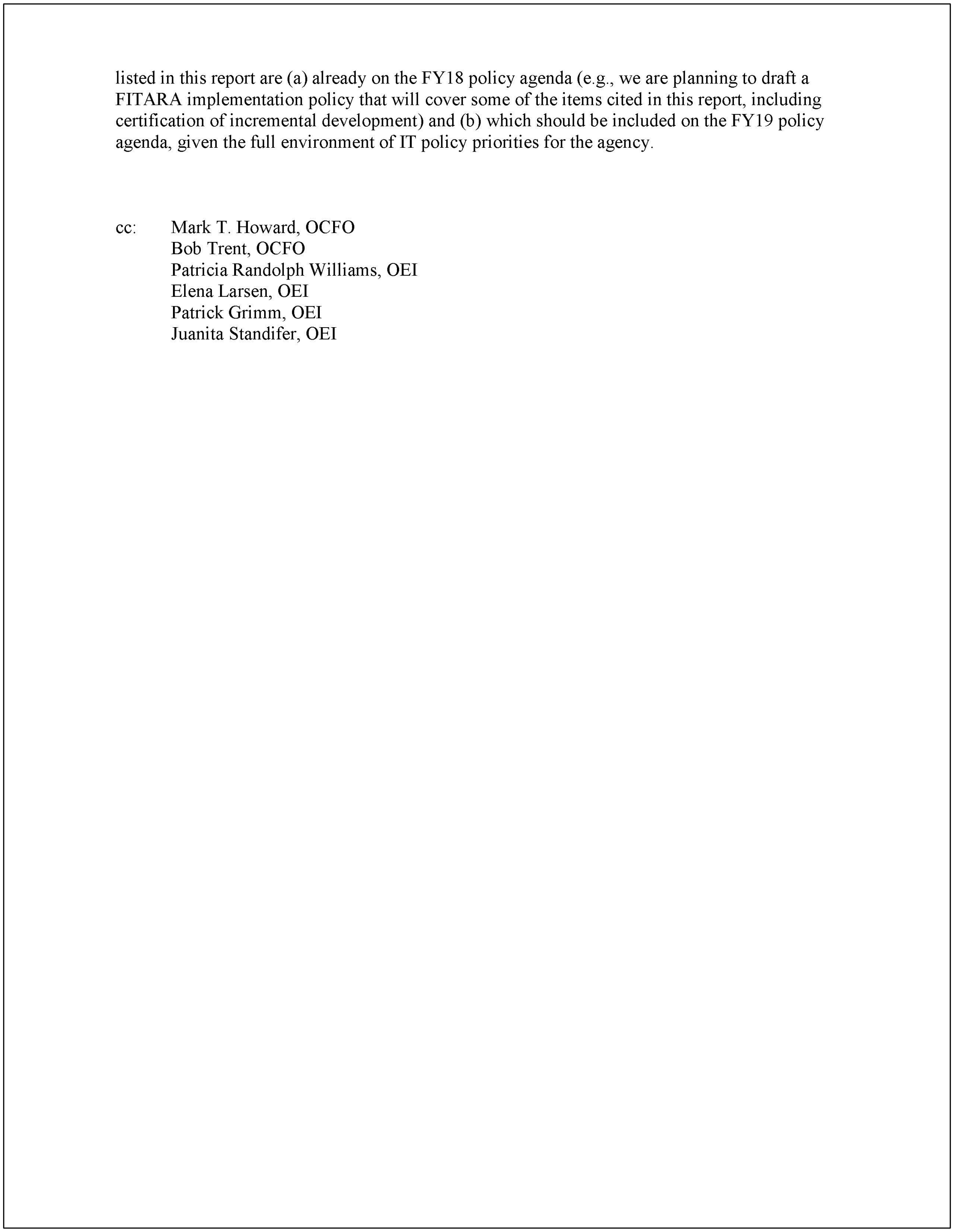
The purpose of this memorandum is to provide EPA's response to the report.

In the Draft Report, GAO recommends that "The Administrator of the Environmental Protection Agency should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 6 areas [GAO] identified".

**Response:**

EPA agrees in principle that CIO authorities should be adequately documented in appropriate policies. This audit documents a large number of CIO authorities that are not yet captured in policy documents. Some of these are items that lack policy or other supporting process or documentation; others have supporting processes in place and simply require a policy statement to formalize the authority. In addition, some require assessment as to whether we are positioned, either from a resource or process ownership perspective, to implement a policy.

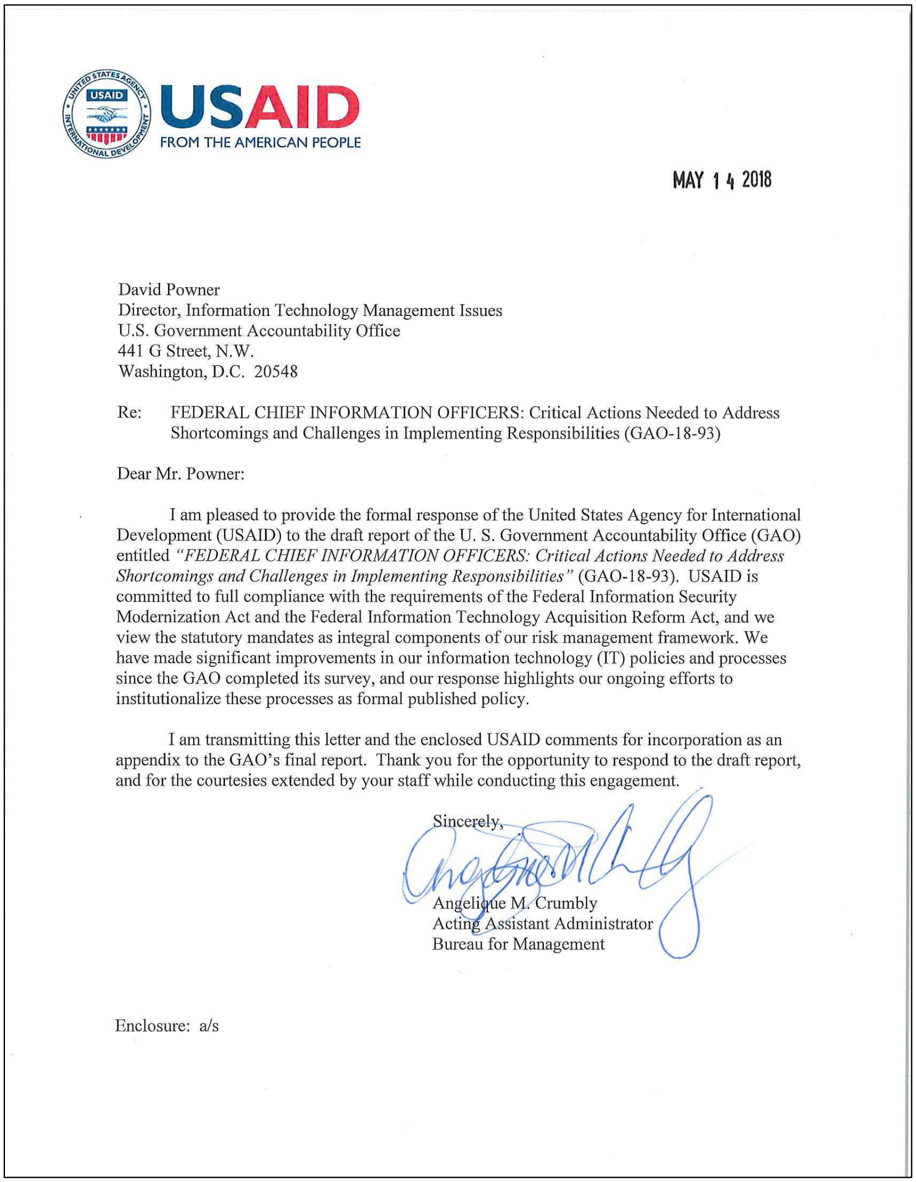
CIO staff, working with Agency senior leaders, set an annual IT policy agenda documenting which policy items will be worked that year. This assures that we devote our resources to the most important policy matters. I will work with my policy staff to determine which of the items



listed in this report are (a) already on the FY18 policy agenda (e.g., we are planning to draft a FITARA implementation policy that will cover some of the items cited in this report, including certification of incremental development) and (b) which should be included on the FY19 policy agenda, given the full environment of IT policy priorities for the agency.

cc: Mark T. Howard, OCFO
Bob Trent, OCFO
Patricia Randolph Williams, OEI
Elena Larsen, OEI
Patrick Grimm, OEI
Juanita Standifer, OEI

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



USAID
FROM THE AMERICAN PEOPLE

MAY 14 2018

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

Re: FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93)

Dear Mr. Powner:

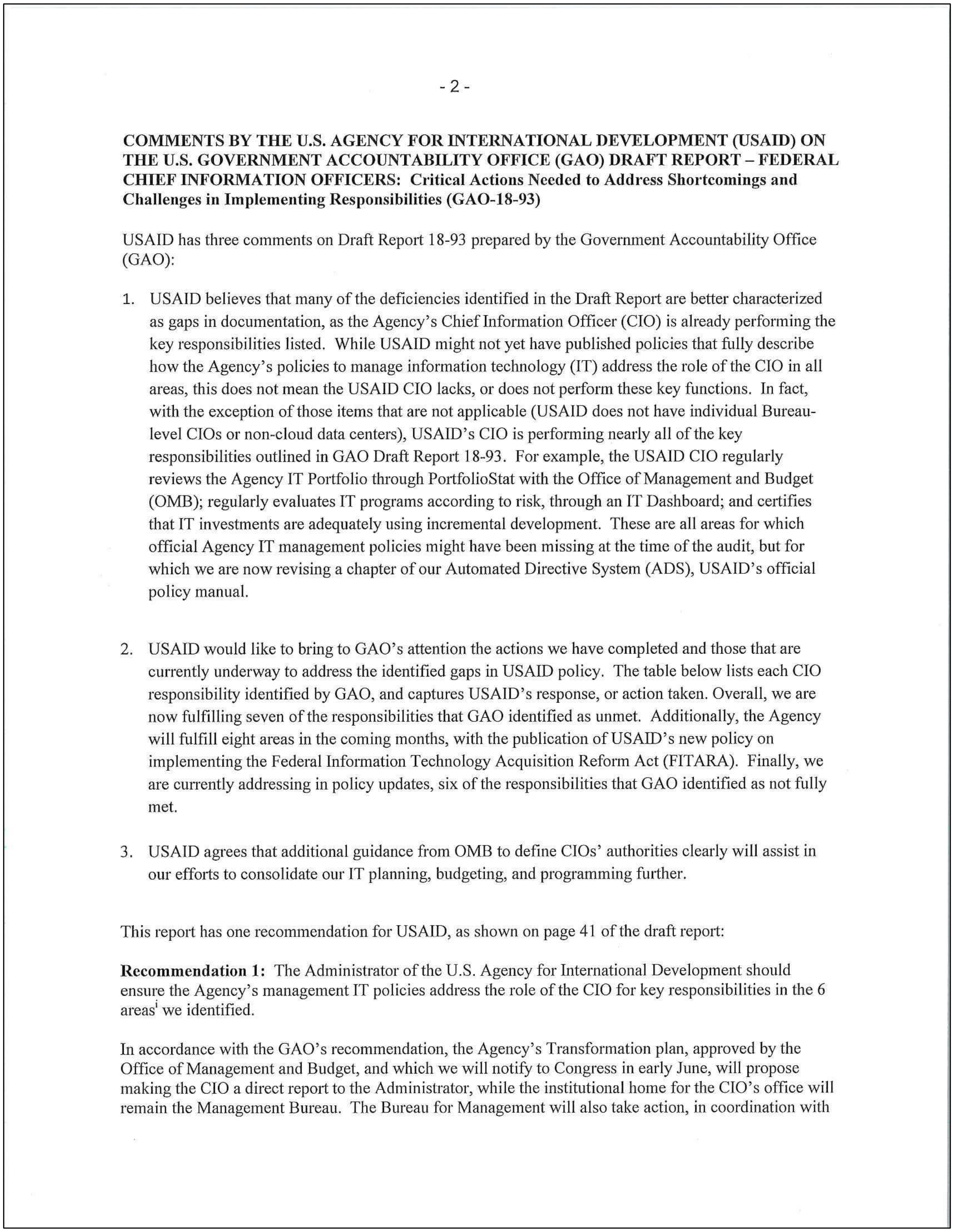
I am pleased to provide the formal response of the United States Agency for International Development (USAID) to the draft report of the U. S. Government Accountability Office (GAO) entitled *"FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities"* (GAO-18-93). USAID is committed to full compliance with the requirements of the Federal Information Security Modernization Act and the Federal Information Technology Acquisition Reform Act, and we view the statutory mandates as integral components of our risk management framework. We have made significant improvements in our information technology (IT) policies and processes since the GAO completed its survey, and our response highlights our ongoing efforts to institutionalize these processes as formal published policy.

I am transmitting this letter and the enclosed USAID comments for incorporation as an appendix to the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

Angelique M. Crumbly
Acting Assistant Administrator
Bureau for Management

Enclosure: a/s



- 2 -

**COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT – FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93)**

USAID has three comments on Draft Report 18-93 prepared by the Government Accountability Office (GAO):

1. USAID believes that many of the deficiencies identified in the Draft Report are better characterized as gaps in documentation, as the Agency's Chief Information Officer (CIO) is already performing the key responsibilities listed. While USAID might not yet have published policies that fully describe how the Agency's policies to manage information technology (IT) address the role of the CIO in all areas, this does not mean the USAID CIO lacks, or does not perform these key functions. In fact, with the exception of those items that are not applicable (USAID does not have individual Bureau-level CIOs or non-cloud data centers), USAID's CIO is performing nearly all of the key responsibilities outlined in GAO Draft Report 18-93. For example, the USAID CIO regularly reviews the Agency IT Portfolio through PortfolioStat with the Office of Management and Budget (OMB); regularly evaluates IT programs according to risk, through an IT Dashboard; and certifies that IT investments are adequately using incremental development. These are all areas for which official Agency IT management policies might have been missing at the time of the audit, but for which we are now revising a chapter of our Automated Directive System (ADS), USAID's official policy manual.

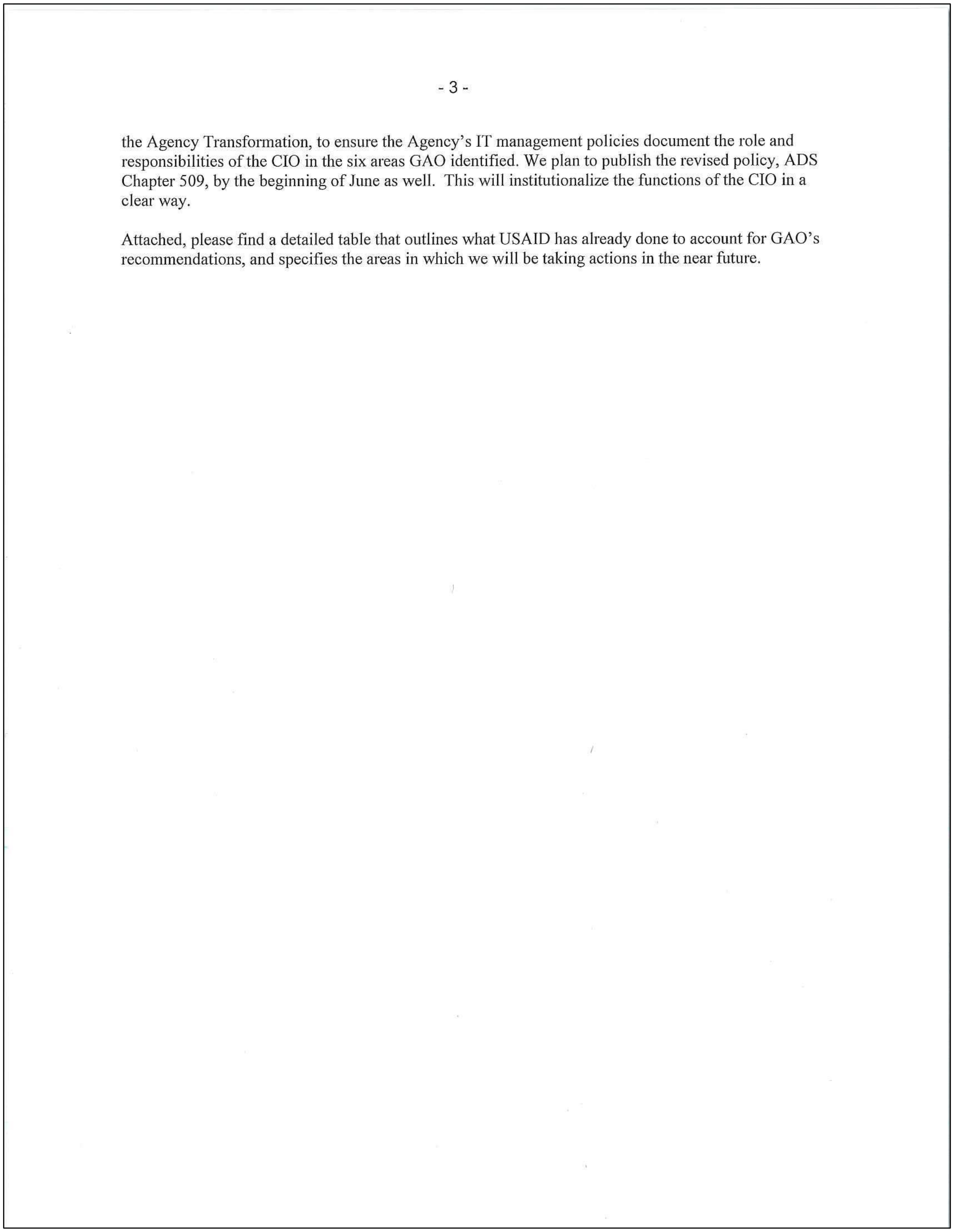
2. USAID would like to bring to GAO's attention the actions we have completed and those that are currently underway to address the identified gaps in USAID policy. The table below lists each CIO responsibility identified by GAO, and captures USAID's response, or action taken. Overall, we are now fulfilling seven of the responsibilities that GAO identified as unmet. Additionally, the Agency will fulfill eight areas in the coming months, with the publication of USAID's new policy on implementing the Federal Information Technology Acquisition Reform Act (FITARA). Finally, we are currently addressing in policy updates, six of the responsibilities that GAO identified as not fully met.

3. USAID agrees that additional guidance from OMB to define CIOs' authorities clearly will assist in our efforts to consolidate our IT planning, budgeting, and programming further.

This report has one recommendation for USAID, as shown on page 41 of the draft report:

**Recommendation 1:** The Administrator of the U.S. Agency for International Development should ensure the Agency's management IT policies address the role of the CIO for key responsibilities in the 6 areas[i] we identified.

In accordance with the GAO's recommendation, the Agency's Transformation plan, approved by the Office of Management and Budget, and which we will notify to Congress in early June, will propose making the CIO a direct report to the Administrator, while the institutional home for the CIO's office will remain the Management Bureau. The Bureau for Management will also take action, in coordination with



the Agency Transformation, to ensure the Agency's IT management policies document the role and responsibilities of the CIO in the six areas GAO identified. We plan to publish the revised policy, ADS Chapter 509, by the beginning of June as well. This will institutionalize the functions of the CIO in a clear way.

Attached, please find a detailed table that outlines what USAID has already done to account for GAO's recommendations, and specifies the areas in which we will be taking actions in the near future.

# Appendix XXVI: GAO Contacts and Staff Acknowledgments

## GAO Contacts

David A. Powner, (202) 512-9286 or pownerd@gao.gov.
Carol C. Harris, (202) 512-4456 or harriscc@gao.gov.

## Staff Acknowledgments

In addition to the contacts named above, individuals making contributions to this report included Nick Marinos (Director), Kevin Walsh (Assistant Director), Kaelin Kuhn (Analyst in Charge), Andrew Beggs, Kiana Beshir, Christopher Businsky, Shaun Byrnes, Rebecca Eyler, David Plocher, Meredith Raymond, Richard Sayoc, Michael Silver, Andrew Stavisky, Tina Torabi, and Theodore Williams.

(101056)

# Appendix XXVII: Accessible Data

## Data Tables

### Data Table for Figure 1: Extent to Which 24 Agencies' Policies Addressed the Role of Their Chief Information Officers, Presented from Most Addressed to Least Addressed Area

| Area | Fully Met | Substantially Met | Partially Met | Minimally Met | Not Met |
|---|---|---|---|---|---|
| Information Technology (IT) leadership and accountability | 11 | 7 | 6 | 0 | 0 |
| IT budgeting | 3 | 9 | 11 | 1 | 0 |
| Information security | 2 | 12 | 10 | 0 | 0 |
| IT investment management | 0 | 3 | 14 | 7 | 0 |
| IT strategic planning | 0 | 1 | 10 | 5 | 8 |
| IT workforce | 0 | 1 | 5 | 6 | 12 |

### Data Table for Figure 2: Extent to Which Chief Information Officers Reported Effective Implementation of Six Responsibility Areas, Presented from Most Effective to Least Effective Area

| Responsibility | Very Effective | Somewhat effective | Slightly effective | Not at all effective | No response |
|---|---|---|---|---|---|
| Information security | 13 | 9 | 1 | 0 | 1 |
| IT planning, programming, and budgeting | 13 | 8 | 2 | 0 | 1 |
| IT leadership and accountability | 11 | 10 | 2 | 0 | 1 |
| IT investment management | 9 | 12 | 2 | 0 | 1 |
| IT strategic planning | 5 | 12 | 6 | 0 | 1 |
| IT workforce | 4 | 11 | 6 | 2 | 1 |

### Data Table for Figure 3: Factors Commonly Identified as Enabling and Challenging Chief Information Officers (CIO) to Effectively Manage Information Technology (IT), Presented from Most Enabling to Least Enabling Factor

| Factor | Major Challenging Factor | Minor Challenging Factor |
|---|---|---|
| National Institute of Standards and Technology guidance | 0 | -3 |
| CIO position in agency hierarchy | -3 | -2 |
| Office of Management and Budget guidance | -4 | -4 |
| Coordination with the Chief Acquisition Officer or his/her office | -4 | -2 |
| Legal authority | 0 | -4 |
| Financial resources | -14 | -3 |
| Availability of personnel/staff resources | -12 | -7 |
| Processes for hiring, recruiting, and retaining IT personnel | -17 | -3 |

| Factor | Major Enabling Factor | Minor Enabling Factor |
|---|---|---|
| National Institute of Standards and Technology guidance | 14 | 3 |
| CIO position in agency hierarchy | 13 | 4 |
| Office of Management and Budget guidance | 13 | 3 |
| Coordination with the Chief Acquisition Officer or his/her office | 12 | 6 |
| Legal authority | 12 | 2 |
| Financial resources | 3 | 3 |
| Availability of personnel/staff resources | 3 | 1 |
| Processes for hiring, recruiting, and retaining IT personnel | 1 | 0 |

**Data Table for Figure 7: Extent to Which 24 Selected Agencies' Policies Addressed the Role of Their Chief Information Officers (CIO), Presented from Most Addressed to Least Addressed Area**

| Area | Fully Met | Substantially Met | Partially Met | Minimally Met | Not Met |
|---|---|---|---|---|---|
| Information Technology (IT) leadership and accountability | 11 | 7 | 6 | 0 | 0 |
| IT budgeting | 3 | 9 | 11 | 1 | 0 |
| Information security | 2 | 12 | 10 | 0 | 0 |
| IT investment management | 0 | 3 | 14 | 7 | 0 |
| IT strategic planning | 0 | 1 | 10 | 5 | 8 |
| IT workforce | 0 | 1 | 5 | 6 | 12 |

**Data Table for Figure 8: Extent to Which 24 Selected Agencies' Policies Addressed the Role of Their Chief Information Officers (CIOs), Presented from Most Addressed to Least Addressed Responsibility**

| Responsibility | Fully addressed | Partially addressed | Not addressed | Not applicable |
|---|---|---|---|---|
| Ensure personnel are trained to effectively carry out information security policies | 24 | 0 | 0 | 0 |
| Develop an agency-wide information security program | 23 | 1 | 0 | 0 |
| Assume responsibility for IT investments | 22 | 0 | 2 | 0 |
| Designate a senior agency information security officer | 22 | 0 | 2 | 0 |
| Implement a process for selecting IT investments | 21 | 2 | 1 | 0 |
| Implement a process for controlling and evaluating IT investments | 21 | 2 | 1 | 0 |
| Develop information security policies and procedures | 20 | 3 | 1 | 0 |
| Review and approve the IT budget request. | 16 | 5 | 3 | 0 |
| Establish goals for improving agency operations through IT | 15 | 0 | 9 | 0 |
| Advise the agency head on underperforming IT investments | 14 | 3 | 7 | 0 |
| Report directly to the agency head | 14 | 0 | 10 | 0 |
| Review and approve funding reprogramming requests | 13 | 0 | 10 | 1 |
| Report to the agency head on the information security program | 12 | 4 | 8 | 0 |

| Responsibility | Fully addressed | Partially addressed | Not addressed | Not applicable |
|---|---|---|---|---|
| Review high-risk IT investments using TechStat sessions | 12 | 1 | 11 | 0 |
| Evaluate IT investments according to risk | 12 | 1 | 11 | 0 |
| Measure performance of how well IT supports programs | 12 | 0 | 12 | 0 |
| Approve the selection of bureau CIOs | 10 | 0 | 3 | 11 |
| Improve the IT portfolio through PortfolioStat | 9 | 0 | 15 | 0 |
| Provide input into bureau CIO performance evaluations | 9 | 0 | 5 | 10 |
| Review and approve IT acquisition plans or strategies | 8 | 9 | 6 | 1 |
| Ensure that senior agency officials carry out their information security responsibilities | 6 | 0 | 18 | 0 |
| Certify that IT investments are adequately implementing incremental development | 5 | 10 | 9 | 0 |
| Assess IT management knowledge and skill requirements | 4 | 6 | 14 | 0 |
| Help ensure that the financial systems are effectively implemented | 4 | 1 | 19 | 0 |
| Have a significant role in IT planning, programming, and budgeting decisions | 3 | 20 | 0 | 1 |
| Prepare an annual report on the progress in achieving the goals | 4 | 0 | 20 | 0 |
| Ensure accountability for information security program compliance | 3 | 0 | 21 | 0 |
| Maintain an inventory of data centers. | 3 | 0 | 19 | 2 |
| Maintain strategy to consolidate and optimize data centers | 2 | 0 | 20 | 2 |
| Ensure processes are analyzed before making significant IT investments | 2 | 0 | 22 | 0 |
| Develop strategies for hiring and training | 1 | 7 | 16 | 0 |
| Report to the head of the agency on IT personnel capabilities progress | 1 | 1 | 22 | 0 |
| Have a significant role in IT governance | 0 | 23 | 0 | 1 |
| Assess whether agency personnel meet IT management knowledge and skill requirements | 0 | 5 | 19 | 0 |
| Benchmark processes against private and public sector performance | 0 | 1 | 23 | 0 |

**Data Table for Figure 9: Extent to Which Agency Chief Information Officers (CIO) Reported Effective Implementation of Six Responsibility Areas, Presented from Most Effective to Least Effective Area**

| Responsibility | Very Effective | Somewhat Effective | Slightly Effective | Not at all Effective | No Response |
|---|---|---|---|---|---|
| Information security | 13 | 9 | 1 | 0 | 1 |
| IT planning, programming, and budgeting | 13 | 8 | 2 | 0 | 1 |
| IT leadership and accountability | 11 | 10 | 2 | 0 | 1 |
| IT investment management | 9 | 12 | 2 | 0 | 1 |
| IT strategic planning | 5 | 12 | 6 | 0 | 1 |
| IT workforce | 4 | 11 | 6 | 2 | 1 |

**Data Table for Figure 10: Extent to Which 24 Chief Information Officers (CIO) Reported Factors as Enabling and Challenging, Presented from Most Enabling to Least Enabling Factor**

| Factor | Major Challenging Factor | Minor Challenging factor | Major Enabling Factor | Minor Enabling Factor |
|---|---|---|---|---|
| National Institute of Standards and Technology guidance | 0 | -3 | 14 | 3 |
| CIO position in agency hierarchy | -3 | -2 | 13 | 4 |
| Office of Management and Budget guidance | -4 | -4 | 13 | 3 |
| Coordination with the Chief Acquisition Officer or his/her office | -4 | -2 | 12 | 6 |
| Legal authority | 0 | -4 | 12 | 1 |
| Coordination with the Chief Financial Officer or his/her office | -1 | -2 | 11 | 7 |
| Delegation of responsibilities | -1 | -3 | 10 | 5 |
| Policy writing authority | 0 | -2 | 9 | 7 |
| Coordination with bureau CIOs | -2 | 0 | 9 | 2 |
| Institutional knowledge at the agency | -1 | -2 | 8 | 9 |
| Coordination with the Chief Human Capital Officer or his/her office | -2 | -5 | 8 | 7 |
| Agency directives | 0 | -2 | 8 | 6 |
| Agency procedures | -1 | -4 | 7 | 8 |
| Prioritization of agency operations and IT needs | -4 | -6 | 7 | 5 |
| Information provided from internal organizations | -2 | -6 | 6 | 5 |
| Coordination elsewhere in the agency | -3 | -6 | 5 | 5 |
| Oversight of indirect reports | -5 | -5 | 5 | 3 |
| Ability to coordinate with external agencies | 0 | -1 | 4 | 7 |
| Level of IT staff expertise | -7 | -9 | 4 | 3 |
| Oversight of IT contractors | -1 | -6 | 4 | 2 |
| Financial resources | -14 | -3 | 3 | 3 |
| Availability of personnel/staff resources | -12 | -7 | 3 | 1 |
| Organizational culture at agency | -7 | -9 | 2 | 5 |
| Processes for hiring, recruiting, and retaining IT personnel | -17 | -3 | 1 | 0 |
| Information provided from contractors & contractor systems | -4 | -3 | 0 | 5 |

**Data Table for Figure 11: Factors Commonly Identified by at Least Half of the Selected Chief Information Officers (CIO) as Enabling Their Effective Management of Information Technology (IT), Presented from Most Enabling to Least Enabling Factor**

| Factor | Major Challenging Factor | Minor Challenging factor | Major Enabling Factor | Minor Enabling Factor |
|---|---|---|---|---|
| National Institute of Standards and Technology guidance | 0 | -3 | 14 | 3 |
| CIO position in agency hierarchy | -3 | -2 | 13 | 4 |
| Office of Management and Budget guidance | -4 | -4 | 13 | 3 |
| Coordination with the Chief Acquisition Officer or his/her office | -4 | -2 | 12 | 6 |
| Legal authority | 0 | -4 | 12 | 2 |

**Data Table for Figure 12: Factors Commonly Identified by at Least Half of the Selected Chief Information Officers (CIO) as Challenges to Their Effective Management of Information Technology (IT), Presented from Most Challenging to Least Challenging Factor**

| Availability of personnel/staff resources | Financial resources | Processes for hiring, recruiting, and retaining IT personnel |
|---|---|---|
| -12 | -14 | -17 |
| -7 | -3 | -3 |
| 3 | 3 | 1 |
| 1 | 3 | 0 |

# Agency Comment Letter

## Text of Appendix VI: Comments from the Department of Agriculture

### Page 1

The U.S. Department of Agriculture (USDA) overall agrees with the finding and recommendation that a Departmental policy be issued to address CIO authorities in the areas identified in the Federal Information Technology Acquisition Reform Act (FITARA). However, USDA has made great strides in the implementation of the Act and has embraced the responsibilities, authorities and accountability provided to the Chief Information Officer (CIO) with the passing of FITARA.

In accordance with Office of Management and Budget (OMB) Memorandum, M-15-14, Management and Oversight of Federal Information Technology, USDA established a Common Baseline

Implementation Plan. USDA has executed over 90% of the Plan requirements and recently, GAO identified USDA as having effective practices in the areas of Federal Data Center Consolidation Initiative (FDCCI) and Category Management/Software Licensing management. Although the USDA CIO does not report directly to the Secretary or Deputy Secretary as specified in M-15-14, the CIO has direct access to the Secretary and Deputy Secretary on all matters pertaining to Information Technology (IT) within USDA and routinely meets with both the Secretary and Deputy Secretary to keep them apprised of all aspects of IT across the USDA IT Portfolio.

To address the recommendation, USDA has established an Integrated Process Team (IPT) with the purpose of updating the USDA FITARA policy to address CIO authorities for IT Leadership, IT Budgeting, IT Investment Management, IT Workforce, IT Strategic Planning and Information Security.

USDA also implemented the Information Technology Management Maturity Model (ITMMM), which focuses on IT Governance, IT Budget, IT Acquisition, Organization and IT Workforce and IT Program Management, to assess the maturity of IT Management within USDA, identify gaps, establish corrective action plans and monitor the maturity levels of IT management going forward. USDA has a plan in place to achieve ITMMM Level 3 (Demonstrative Maturity).

## Text of Appendix VII: Comments from the Department of Commerce

Page 1

Dear Mr. Powner:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93).

On behalf of the Department of Commerce, I have enclosed our response on the draft report.

We concur with GAO's recommendation and will work to timely develop a plan to ensure the Department's information technology (IT) management policies clearly and fully address the role of the Department's chief information officer in the five areas: (1) IT Strategic Planning, (2) IT Workforce, (3) IT Budgeting, (4) IT Investment Management, and (5) Information Security.

If you have any questions, please contact MaryAnn Mausser, the Department's GAO Liaison, at (202) 482-8120.

Sincerely,

Wilbur Ross

Enclosures

Page 2

**Department of Commerce's Comments on GAO Draft Report titled Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GA0-18-93)**

The Department of Commerce has reviewed the draft report, and we offer the following comments for the Government Accountability Office's (GAO) consideration.

**Comments on Recommendations**

GAO made one recommendation to the Department in the report:

**Recommendation 1:**

The Secretary of Commerce should ensure that the Department's IT Management policies address the role of the CIO for key responsibilities in the five areas we identified.

**Commerce Response:**

We concur with GAO's recommendation and will work to timely develop a plan to ensure the Department's IT management policies clearly and fully address the role of the Department's CIO in the five areas: (1) IT Strategic Planning, (2) IT Workforce, (3) IT Budgeting, (4) IT Investment Management, and (5) Information Security.

# Text of Appendix VIII: Comments from the Department of Education

Page 1

Dear Mr. Powner:

I am pleased to provide the U.S. Department of Education's (ED's or Department's) response to the Government Accountability Office's (GAO's) draft report GAO-18-93, Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities. We understand that GAO conducted this audit to determine whether the Department has sufficient, documented policies to address the role of the agency Chie f Information Officer (CIO) for the responsibilities listed in Table I: Summary of Key Chief Information Office r (C /0 ) Responsibilities consistent with federal la w and Office of Management and Budget (OMB) guidance. We appreciate the opportunity to respond to the recommendations in this draft GAO report.

**Recommendation 7:**

The Secretary of Education should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified.

**Response:**

The Department concurs with the findings and the recommendations of GAO. In response to the major legislative directives involving the CIO ' s responsibilities, the Department developed: (i) the Delegation of authority to perform all functions vested by the Information Technology Management Reform Act (IT MRA) of 1996, (ii) the Delegation of authority to perform all tasks as described under Federal Information Technology Management Reform Act (FITARA) of 2014, and (iii) various policy documents provided to GAO as part of this study to describe the agency C IO ' s role in the responsibilities listed in Table I: Summary of Key Chief Information Officer (C/0) Responsibilities. These documents were developed to empower the CIO to execute all tasks as described in federal law and OMB guidance. The Department's CIO is currently performing most of the responsibilities enumerated in this study. However, we recognize that the responsibilities are not explicitly documented in our policies, and we plan to update these policies to reflect the specific requirements identified by GAO.

Page 2

As part of maturing agency policies under our FITARA implementation initiative, the Department is updating and developing agency policies to address the role of the CIO for key responsibilities in the five areas GAO identified and as listed in Table 8: Extent to Which Department of Education Policies Addressed the Role of/is Chief Information Officer on pages 60-61 of GAO-18-93.

If you have any questions, please contact Walter McDonald, Director of Information Technology Program Services, at (202) 245-6794 or at Walter.McDonald@cd.gov.

Sincerely,

Jason K. Gray

## Text of Appendix IX: Comments from the Department of Energy

Page 1

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-18-93, Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (Job Code 101056). We understand that GAO conducted this audit to (1) dete1mine the extent to which DOE has defined the role of the Chief Information Officer (CIO) in accordance with federal law and guidance and (2) describe key challenges of the CIO in fulfilling the responsibilities to carry out federal law and guidance. The GAO had the following recommendation for DOE:

**Recommendation:**

The Secretary of Energy should ensure that the department's IT management policies address the role of the C/O for key responsibilities in the 5 areas we identified.

**Management Response:**

Concur

DOE is working diligently to implement the responsibilities of the CIO as required by law. DOE will ensure that the department's IT management documents and/or policies address the role of the CIO for key responsibilities in the 5 areas that the GAO identified in table 9 of this report. DOE expects to complete the documentation process by May JS', 2019.

You may direct your questions to Mr. Nils Johanson, Acting Deputy CIO, Office of Enterprise Policy, Portfolio Management, and Governance at 202-586-9949 or via e-mail to Nils.johanson@hq.doe.gov.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

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

Page 1

Dear Mr. Pawner:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" (GAO-18-93).

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

Sincerely,

Matthew D. Bassett
Assistant Secretary for Legislation

Attachment

Page 2

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

**Recommendation 1**

The Secretary of HHS should ensure that the department’s Information Technical (IT) management policies address the role of the Chief Information Officer (CIO) for key responsibilities in the 6 areas we identified.

**HHS Response**

HHS concurs with GAO’s recommendation.

HHS has made significant progress in ensuring the CIO authorities per Federal Information Technology Acquisition Reform Act (FITARA). The findings outlined on pages 64 and 65 of the draft report should show the following (i.e., full Harvey balls):

**Responsibility**

Approve the selection of bureau CIOs.

Measure how well IT supports agency programs.

Prepare an annual repo1t on the progress in achieving the goals.

Assess annually the requirements established for agency personnel regarding IT management knowledge and skills.

Assess annually the extent to which agency personnel meet IT management.

Knowledge and skill requirements have a significant role in IT planning, programming, and budgeting decisions.

Review and approve the IT budget request.

Review and approve funding reprogramming requests Improve the management of the agency’s IT through portfolio review (Portfolio Stat).

Evaluate IT investments according to risk (IT Dashboard CIO Ratings).

Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget (OMB).

Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented.

Maintain an inventory of data centers.

Ensure that senior agency officials, including CIOs of bureaus or equivalent officials carry out their information security responsibilities.

Page 3

Ensure that all personnel are held accountable for complying with the agency-wide information security program.

HHS has acted to address the abovementioned areas of CIO responsibility:

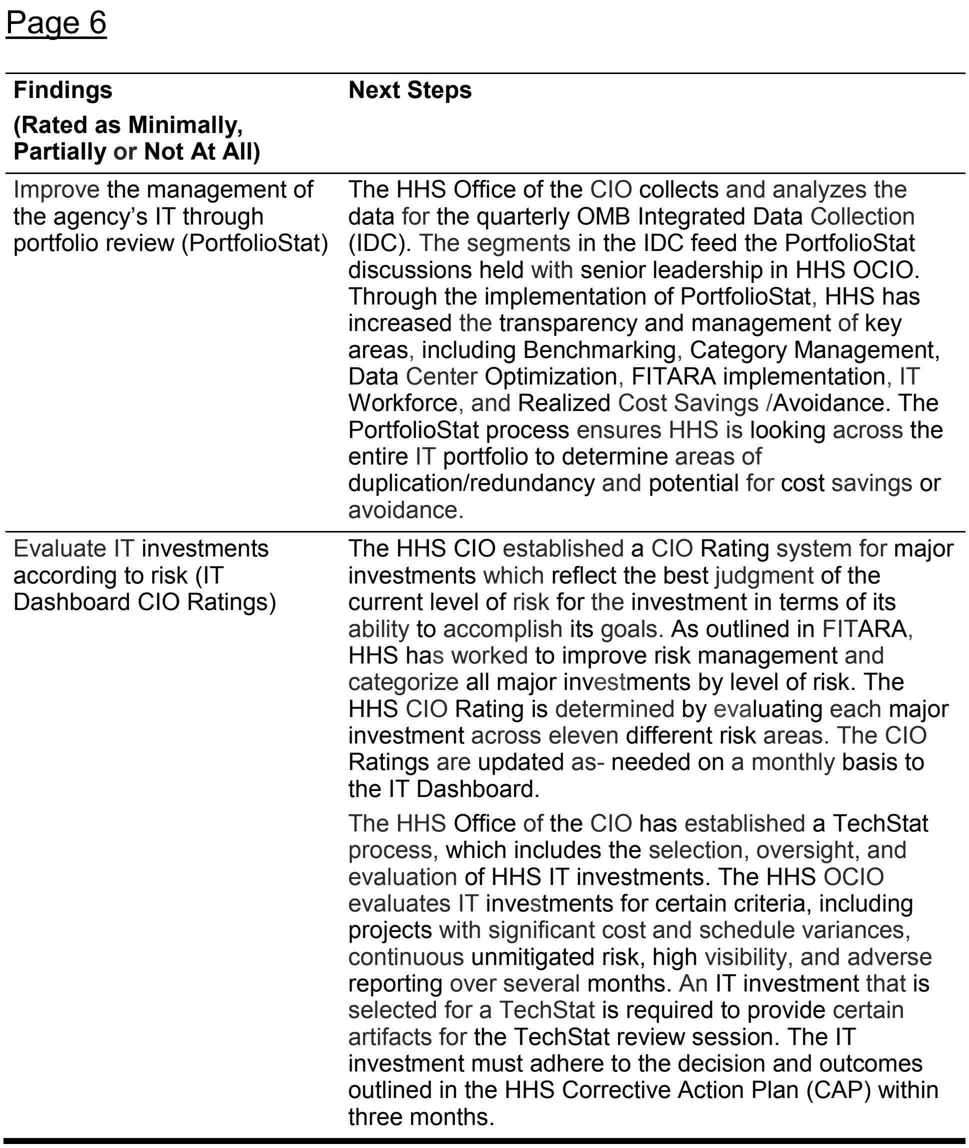
| Findings<br>(Rated as Minimally, Partially or Not At All) | Next Steps |
|---|---|
| Approve the selection of bureau CIOs | The HHS CIO participates in the hiring and evaluation of bureau (Operating Divisions) CIOs. The policy is attached. |
| Measure how well IT supports agency programs | The HHS OCIO is working in tandem with the Assistant Secretaries for Administration (ASA) and Planning and Evaluation (ASPE) on Performance Management that includes IT and cybersecurity related goals, objectives and key performance indicators per several key documents: (1) HHS Strategic Plan; the (2) HHS Information Technology Strategic Plan, and the (3) President's Management Agenda, issued in April 2018. |
| Prepare an annual report on the progress in achieving the goals | As part of Performance Management described above, the HHS OCIO in tandem with ASA and ASPE will establish IT and cybersecurity benchmarks in 2018 (if they have not been already established), and measure progress on an annual basis. |
| Assess annually the requirements established for agency personnel regarding IT management knowledge and skills | The HHS Office of Chief Information Officer (OCIO) and Office of Human Resources (OHR) continue their partnership to comprehensively address HHS IT workforce business needs and legislative requirements while improving the Department's ability to attract, develop, and retain IT talent.<br>As required by law, HHS uses the National Institute of Standards and Technology (NIST)/NICE Framework (SP 800-181) to annually assess our current workforce capabilities. HHS is also required by law to use the 2210 IT Management Occupational Series for determining the qualification requirements of our IT Management Workforce when hiring or promoting staff.<br>While working with OHR to harmonize the NIST 800-181 requirements and the 2210 qualification standards, the Department is developing mitigation strategies for closing gaps in its critical IT and cybersecurity roles. |

Page 4

| Findings<br>(Rated as Minimally, Partially or Not At All) | Next Steps |
|---|---|
| | For example, through a study, HHS identified gaps in knowledge and skills (hence training and certification) of its IT and cybersecurity workforce. HHS training, certification, and skill requirements are also being ascertained through our competency modeling and career pathing efforts (12 of 29 Career Paths and Competency Models have been developed to-date).<br>HHS is also currently assessing its staffing needs through the Federal Cybersecurity Workforce Assessment Act (FCWAA) coding efforts. FCWAA requires Agencies to: (a) identify all encumbered and vacant positions within the agency that require the performance of IT, cybersecurity, or other cyber- related functions; (b) determine whether these individuals have certifications that are commensurate with their IT work, determine the preparedness levels of personnel to achieve certifications if they do not maintain one, and submit a report and mitigation strategy to congress; and (c) assign the corresponding employment code from NIST Special Publication (SP) 800-181 National Cybersecurity Workforce Framework (NCWF).<br>HHS initial coding is due to the Office of Personnel Management (OPM) by April 30, 2018. Agencies are required to annually submit this coding data to OPM until at least 2022. This coding will yield insights into the Department’s IT and cybersecurity staffing requirements. |
| Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements | As discussed earlier, HHS conducted a study to identify gaps in knowledge and skills. The findings of the study are informing training and certification requirements. This activity is complemented by HHS’ FCWAA coding efforts, and competency modeling and career pathing efforts.<br>HHS is working with OPM on its latest Memo for Identifying,<br>Addressing, and Reporting on Work Roles of Critical Need (htt12s: //chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need), |

Page 5

| Findings<br>(Rated as Minimally, Partially or Not At All) | Next Steps |
|---|---|
| | On April 2, 2018, OPM provided guidance on how agencies will identify, address, and report on their greatest skill shortages by April 2019 (e.g., identify root causes for shortages, develop mitigation/action plans, and metrics).<br>These activities will be foundational to HHS' IT and cybersecurity workforce analyses and resulting, targeted university and workforce recruitment strategies. |
| Have a significant role in IT planning, programming, and budgeting decisions | The HHS CIO continues to delegate the authority for IT decision-making related to planning, programming, and budgeting to each of the Operating Divisions CIOs. At a higher level, however, the decisions for major IT investments ($20M, annually, and above) are reviewed through the annual IT budget review process.<br>In this process, the HHS Chief Financial Officer (CFO) and HHS CIO play a role in reviewing planned IT support for major programs, including assessing the impact of significant changes in IT resources as reflected in the IT budget. |
| Review and approve the IT budget request | The HHS CIO reviews and provides input into approving IT investments as evident in the HHS annual IT Budget review process that involves high-level planning and programming. Furthermore, both the HHS CFO and HHS CIO play a role in reviewing planned IT support for major programs and significant increases and decreases in IT resources as reflected in the IT budget. |
| Review and approve funding reprogramming requests | The HHS CIO continues to review and approve IT funding reprogramming requests through the Capital Planning and Investment Control (CPIC) process.<br>As outlined by CPIC policy:<br>A Performance Management Baseline shall be established for each IT Investment with Development, Modernization, and Enhancement activities.<br>The IT Investment manager shall report, monitor, and implement actions as needed to correct variances from established IT Investment baselines to reduce the risk of cost overruns, schedule delays, and uncontrolled changes m scope.<br>Any deviations from the baseline must documented through a baseline change request and have review/approval from the appropriate IT Governance board. These can include missed milestones and/or variances in percentage of project cost, schedule, or performance outside any defined acceptable ranges. |



Page 6

| Findings<br>(Rated as Minimally, Partially or Not At All) | Next Steps |
|---|---|
| Improve the management of the agency's IT through portfolio review (PortfolioStat) | The HHS Office of the CIO collects and analyzes the data for the quarterly OMB Integrated Data Collection (IDC). The segments in the IDC feed the PortfolioStat discussions held with senior leadership in HHS OCIO. Through the implementation of PortfolioStat, HHS has increased the transparency and management of key areas, including Benchmarking, Category Management, Data Center Optimization, FITARA implementation, IT Workforce, and Realized Cost Savings /Avoidance. The PortfolioStat process ensures HHS is looking across the entire IT portfolio to determine areas of duplication/redundancy and potential for cost savings or avoidance. |
| Evaluate IT investments according to risk (IT Dashboard CIO Ratings) | The HHS CIO established a CIO Rating system for major investments which reflect the best judgment of the current level of risk for the investment in terms of its ability to accomplish its goals. As outlined in FITARA, HHS has worked to improve risk management and categorize all major investments by level of risk. The HHS CIO Rating is determined by evaluating each major investment across eleven different risk areas. The CIO Ratings are updated as- needed on a monthly basis to the IT Dashboard.<br>The HHS Office of the CIO has established a TechStat process, which includes the selection, oversight, and evaluation of HHS IT investments. The HHS OCIO evaluates IT investments for certain criteria, including projects with significant cost and schedule variances, continuous unmitigated risk, high visibility, and adverse reporting over several months. An IT investment that is selected for a TechStat is required to provide certain artifacts for the TechStat review session. The IT investment must adhere to the decision and outcomes outlined in the HHS Corrective Action Plan (CAP) within three months. |

Page 7

| Findings<br>(Rated as Minimally, Partially or Not At All) | Next Steps |
|---|---|
| Certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget | The HHS CIO ensures IT investments with projects are adequately implementing incremental development through the HHS Policy for IT Enterprise Performance Life Cycle (EPLC). All HHS IT projects shall use appropriate, proven development methods to ensure that planned and actual delivery of new or modified technical functionality occurs at least every six months, including but not limited to agile methods to ensure incremental delivery. A project that uses newer, less proven methods must have approval by the appropriate HHS or Bureau IT Governance body. Over 90% of the active projects reported on the IT Dashboard are using incremental development. |
| Coordinate with the agency head and chief financial officer to ensure that the financial systems are effectively implemented | Through the IT budget review process, the HHS Chief Financial Officer (CFO) and HHS CIO play a role in reviewing planned IT support for major programs and significant increases and decreases in IT resources as reflected in the IT budget. This process includes all IT investments/systems including financial systems. |
| Maintain an inventory of data centers | The HHS CIO collects and maintains an inventory of the data centers (tiered and non-tired) across all of HHS through the quarterly OMB IDC. Each bureau within HHS is responsible for collecting, validating and maintaining their data center inventory. The inventory is sent to the HHS CIO for review and approval, before it is sent to the MAX DataPoint Portal. Any cost savings identified through the closure of data centers is also reported through the data center inventory. |
| Ensure that senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities | All HHS staff members and contractors receive security awareness training consistent with Federal Information Security Modernization Act FISMA requirements and guidance from NIST. |
| Ensure that all personnel are held accountable for complying with the agency-wide information security program | As noted, all HHS staff and contractors take security awareness training annually. Additionally, each signs rules of behavior which specifically detail cybersecurity requirements in support of the HHS cybersecurity program. Personnel are held accountable to these and all information security policies as a result of signing these rules. |

Page 8

DATE: 04/27/2016

SUBJECT: Federal IT Acquisition Reform Act- Operational Division Chief Information Officer Evaluations

The Federal Information Technology Reform Act (FITARA) was enacted on December 19, 2014 to improve federal Information Technology (IT) investments. Following passage of FITARA, the Office of Management and Budget (OMB) published implementation guidance (M-15-14) to all federal agencies in June 2015. OMB defined an IT Common Baseline that each agency must address by December 31, 2015. The IT Common Baseline defines standards that agencies must achieve related to four key areas - budget, acquisition, program management and human capital. With this objective, the Department of Health and Human Services (HHS) implementation plan was developed by Assistant Secretary for Financial Resources and Assistant Secretary for Administration under the sponsorship of the acting Deputy Secretary. The purpose of this memorandum is to establish guidance on how to achieve human capital objectives related to the hiring and performance evaluation of personnel with the title or function of Chief Information Officer within HHS. This policy memorandum serves as the official HHS guidance on hiring and evaluating HHS personnel ‘‘with the title and/or function of a Chief Information Officer (CIO) within any segment of the HHS organization.”

### Hiring

Going forward, for any individual within HHS hired with the title and/or function of a CIO, the HHS Department CIO shall play a role in the following staffing activities: participation as a subject matter expert in reviewing candidates, participation in the interview process, and/or participation in the selection process. The Division Head and HHS CIO will mutually agree on the selection of an individual for this type of position.

Page 9

**Performance**

The HHS CIO and Chief Human Capital Officer (CHCO) have chosen the Business Acumen element of the standard Senior Executive Service (SES) Performance Management Annual Plan (PMAP) as the official rating element for Division-level CIO performance on III-IS accountabilities (regardless of whether the position is SES or GS-15). To accommodate other Operating Division (OpDiv) imperatives, the rating official can include additional business acumen accountabilities in the plan provided that the HHS CIO Work Plan component equates to 5% of the overall Performance Plan scoring.

In FY2016 and beyond, the HHS CIO shall provide and discuss with the respective OpDiv CIOs a quarterly Work Plan score for review and comment. The IDIS CIO will provide to respective Division heads, mid-year and annual input for this component of the CIO's PMAP. The Division Head or other rating official of the OpDiv CIO will consider the input from the HHS CIO when determining the initial summary rating and will discuss the input with the Division CIO during progress and final reviews.

The HHS CIO will establish an annual CIO Work Plan, with Operating Division CIO input, that will feed into the Business Acumen element. The Work Plan may vary from year-to-year in the number of accountable items and the weights of items to represent their relative importance towards HHS goals. The CIO Work Plan has been in place for three years and will continue to be used across all HHS Divisions to establish expectations and rate the OpDiv CIOs' performance for this component of the PMAP. The Division head or rating official (if other than the Division head) will determine the overall summary rating for Division-level CIOs.

The development of the CIO Work Plan is a collaborative effort by the CIO Work Plan Working Group, OCIO raters, and feedback from the HHS CIO Council, with the agency CIO holding ultimate authority over the final plan and ratings. The HHS Office of the CIO (OCIO) creates and scores the work plan on a fiscal year (FY) basis to align with SES evaluations. For OpDiv CIOs not within the SES, the final work plan rating for the FY will be used in the calendar year close out. The CIO Work Plan is a scorecard with elements (e.g., OMB PortfolioStat initiatives) that the Department and Division levels must complete. OCIO updates the work plan yearly and provides ratings on a quarterly basis.

Each year the CIO and CHCO will provide a rating cycle, rating criteria for PMAP scoring and copy of the CIO Work Plan Elements to the Operating Division heads.

If you have any questions regarding the CIO Work Plan or its elements, please direct them to the HHS CIO Coordinator at HHSCIOCouncil@HHS.gov.

cc: HHS Deputy Secretary
HHS Acting Assistant Secretary for Administration

## Text of Appendix XI: Comments from the Department of Homeland Security

Page 1

Dear Mr. Powner:

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

The Department is pleased to note GAO's recognition of DHS's policies created to ensure the role of the Chief Information Officer (CIO) is consistent with federal laws and guidance. Subsequent to GAO's issuance of this draft report for management comment, DHS updated and revised the delegation of authority from the Under Secretary for Management to the CIO, (Delegation 04000) explicitly authorizing the CIO to exercise the full range of authorities enumerated in the Federal Information Technology (IT) Acquisition Reform Act and other seminal statutes. In addition, DHS updated Directive 142-02, "Information Technology Integration and Management" to reflect the authority granted by the Delegation. Together, the Delegation and Directive clearly address the CIO responsibilities not fully addressed previously.

The draft report contained 27 recommendations, one that was for DHS and with which the Department concurs. Attached find our detailed response to the recommendation. Technical comments were provided under separate cover.

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

Sincerely,

Director
Departmental GAO-OIG Liaison Office

Attachment

Page 2

### Attachment: Management Response to Recommendation Contained in GA0-18-93

GAO recommended that the Secretary of Homeland Security:

**Recommendation:**

Ensure that the department's information technology IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified. (Recommendation 10)

**Response:**

Concur. The DHS Under Secretary for Management signed Delegation 04000, “Delegation to the Chief Information Officer” and Directive 142-02, “Information Technology Integration, and Management,” on April 30, 2018 and April 12, 2018, respectively. These documents codify in policy the CIO responsibilities enumerated in this report. GAO identified six areas in which federal law imbues agency CIOs with critical duties:

- IT Leadership and Accountability
- IT Strategic Planning
- IT Workforce
- IT Budgeting
- IT Investment Management
- Information Security

Each of these areas contains several distinct responsibilities. GAO found that DHS policy fully supported all of the responsibilities contained in IT Budgeting and the majority of the responsibilities contained in IT Leadership and Accountability, IT Investment Management, and Information Security. However, the policy did not support any of the responsibilities set out under IT Strategic Planning and IT Workforce.

The updated Delegation and Directive now clearly sets out the general CIO responsibilities to encompass the statutory requirements in all six areas identified above. Other guidance addresses more focused CIO responsibilities such as Capital Planning and Investment Control and Portfolio Management.

Copies of the new Delegation and Directive were provided to GAO under separate cover. We request that GAO consider this recommendation resolved and closed, as implemented.

## Text of Appendix XII: Comments from the Department of the Interior

Page 1

Dear Mr. Powner:

Thank you for providing the Department of Interior (Department) the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled, Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93): We appreciate GAO's review of Federal Chief Information Officer authorities.

The Department concurs with recommendation 12 which states: "The Secretary of the Interior should ensure that the Department's Information Technology management policies address the role of the Chief Information Officer (CIO) for key responsibilities in the five areas we identified." The Department believes it has sufficiently addressed the role of the CIO. However, the Department will perform a policy analysis review to verify that the CIO authorities are appropriately implemented in accordance with statute and will take corrective actions as necessary, based on the results of the analysis.

Please incorporate our comments when finalizing the report. If you have any questions or need additional information, please contact Sylvia Burns, Chief Information Officer at Sylvia_Burns@ios.doi.gov.

Sincerely,

Scott J. Cameron
Principal Deputy Assistant Secretary for Policy,
Management and Budget Exercising the Authority of
the Assistant Secretary for Policy, Management and
Budget

## Text of Appendix XIII: Comments from the Department of Veterans Affairs

Page 1

Dear Mr. Powner:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" (GAO-18-93).

The enclosure sets forth the actions to be taken to address the GAO draft report recommendations.

VA appreciates the opportunity to comment on your draft report.

Peter O'Rourke
Chief of Staff

Enclosure

Page 2

**Department of Veterans Affairs (VA) Comments to Government Accountability Office (GAO) Draft Report "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing**

**Responsibilities"**
**(GAO-18-93)**

**Recommendation 1:**

The Secretary of Veterans Affairs should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 4 areas GAO identified

**VA Comment:**

Concur. While the Department of Veterans Affairs (VA) Chief Information Officer is currently implementing most of the responsibilities across the six information technology (IT) management areas identified by GAO in the draft report, VA acknowledges that many of these responsibilities are not explicitly formalized by Departmental policy. In the Department's 60-day update to GAO's final report, VA will outline the specific actions to be taken to address this recommendation. VA is committed to ensuring that the Department's IT management policies fully address all key IT management responsibilities of Federal chief information officers.

## Text of Appendix XIV: Comments from the Department of State

Page 1

Dear Mr. Johnson:

We appreciate the opportunity to review your draft report, "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" GAO Job Code 101056.

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 Paula Lee, IT Specialist, Office of Business Management and Planning, Bureau of Information Resource Management at (202) 653-9756.

Sincerely,

Christopher H. Flaggs

Enclosure:
As stated

cc: GAO - David Powner
IRM - Karen Mummaw (Acting)
OIG- Norman Brown

Page 2

**Department of State Response to the Draft Report**
**FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities**
**(GAO-18-93, GAO Code 101056)**

The Department of State appreciates the opportunity to respond to GAO's draft report entitled "Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities."

The Secretary of State should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 6 areas we identified. (Recommendation 15)

The Department of State concurs with the recommendation. The Department is committed to the on-going policy realignment effort to comply with IT management policies that address the role and responsibilities of the CIO

## Text of Appendix XV: Comments from the National Aeronautics and Space Administration

Page 1

Dear Mr. Powner:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Federal Chief Information Officers:

Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities” (GAO-18-93), dated April 6, 2018.

In the draft report, GAO makes one recommendation to the NASA Administrator intended to improve the effectiveness of Federal Chief Information Officers (CIOs) implementation of their responsibilities relative to the following six information technology (IT) management areas: 1) leadership and accountability; 2) budgeting; 3) security; 4) investment management; 5) workforce planning; and 6) strategic planning.

Specifically, GAO recommends the following:

**Recommendation 1:**

The Administrator of NASA should ensure that the department’s IT management policies address the role of the CIO for key responsibilities in the six areas identified.

**Management’s Response:**

NASA concurs with the recommendation. NASA is currently updating the following policies to address the six areas defined in the GAO report: NASA Policy Directive (NPD) 2800.1, “Managing Information Technology;” and NASA Procedural Requirement (NPR) 7120.7, “NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.”

**Estimated Completion Date:**

January 18, 2019

Page 2

Once again, thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Ruth McWilliams on (202) 358-5125.

Sincerely,

Renee P. Wynn
Chief Information Officer

# Text of Appendix XVI: Comments from the National Science Foundation

Page 1

Dear Mr. Pawner:

Thank you for the opportunity to review and comment on the Government and Accountability Office (GAO) draft report titled Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO 18-93).

On behalf of the National Science Foundation (NSF), I have enclosed our comments on the draft report. NSF concurs with the recommendation and is committed to fully implementing the Federal Information Technology Acquisition Reform Act (FITARA). Since the issuance of this report, NSF has updated the agency IT security policy to provide more specificity about the role of the CIO. We have also provided GAO with documents which articulate the CIO's role in the Budgeting and IT Investment Management areas detailed in this engagement; highlighted in the enclosure.

NSF is committed to implementing appropriate improvements to ensure that the Foundation maintains sound IT management policies and appreciates GAO's work and continued interest in this area. If you have any questions, please contact Veronica Shelley, NSF Liaison to the GAO, at (703)-292-4384 or vshelley@nsf.gov.

Sincerely,

Dorothy Aronson<br>Chief Information Officer

Enclosure

Page 2

**Recommendation 22:**

The Director of the National Science Foundation should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified."

**NSF Response:**

NSF concurs with the recommendation, and will ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas identified by GAO. The following evidence has been provided:

- The Proposed IT Investment Form and Business Case Form to ensure processes are analyzed and revised as appropriate before making significant IT investments
- The IT Resource Statement to ensure the CIO has a significant role in IT planning, programming, and budgeting decisions
- The IT Resource Statement also certifies that IT investments are adequately implementing incremental development, as defined in the capital planning guidance issued by OMB
- The Reprogramming Process to review and approve agency reprogramming requests
- The position description of the CIO describes the CIO's role in advising the Director in all matters related to IT
- The NSF DCOI inventory maintains an inventory of data centers
- The NSF DCOI Strategic Plan maintains the strategy to consolidate and optimize data centers
- The updated Information Security Handbook ensures that senior agency officials, including the CIO, carry out their information security responsibilities; and that all personnel are held accountable for complying with the agency-wide information security program

## Text of Appendix XVII: Comments from the Office of Personnel Management

Page 1

Dear Mr. Powner:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, entitled Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities, GAO-18-93, GAO Job code 101056.

Our response to your recommendation is provided below.

Recommendation #1: The Director of the Office of Personnel Management should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 areas we identified.

Management Response:

We concur. OPM will review and update, as appropriate, the agency's IT management policies to address the role of the CIO for the key responsibilities identified.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Ashu Goel, Associate CIO for Strategy & Policy, (202) 418-4326, and Ashu.Goel@opm.gov.

Sincerely,

Dr. Jeff T.H. Pon

## Text of Appendix XVIII: Comments from the Social Security Administration

Page 1

Dear Mr. Powner:

Thank you for the opportunity to review the draft report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities" (GAO-18-93). Please see our attached comments.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director for the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall
Acting Deputy Chief of Staff

Attachment

Page 2

**SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES" (GAO-18-93)**

SSA continues to make progress in integrating our Chief Information Officer (CIO) into managing the areas of Information Technology (IT) Strategic Planning, IT Workforce, IT Budgeting, and IT Investment Management. While we acknowledge the report's findings, we have initiated a timeline to attain full compliance in all six of the key IT management areas identified by GAO. As we continue to integrate the CIO in our management practices, we are developing a formal policy that addresses the CIO's responsibilities in the five areas that GAO noted we are not fully compliant.

In March 2018, we completed the first iteration of our new CIO policy and addressed the CIO's responsibilities relating to IT Leadership and Accountability, IT Strategic Planning, and IT Budgeting, and some of the responsibilities related to IT Investment Management.

We are finalizing the second iteration of the policy, which includes the remaining IT Investment Management responsibilities. We expect to have a completed CIO directive that fully addresses all six areas of responsibility by September 30, 2018.

In addition to the high-level directive, we created lower-level CIO Responsibility policies for the Certification of Incremental Development and IT Acquisition Approval.

Below is our response to the recommendation.

**Recommendation 1**

Ensure that the department's IT management policies address the role of the CIO for key responsibilities in the six areas it identified.

**Response**

We agree.

## Text of Appendix XIX: Comments from the Department of Defense

Page 1

Dear Mr. Powner:

This is the Department of Defense (DoD) response to the GAO Draft Report, GA0-18-

93, "FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities'' dated April 6, 2018 (GAO Code 101056). Enclosed is DoD's proposed response to the subject report. My point of contact for this matter is Mr. Craig Garant, (703) 697-1029, craig.r.garant.civ@mail.mil.

Sincerely,

Essye W. Miller
Principal Deputy

Enclosure: As stated

Page 2

**ATTACHMENT**
**GAO DRAFT REPORT DATED APRIL 6, 2018 GAO-18-93 (GAO CODE 101056) "FEDERAL CHIEF INFORMATION OFFICERS: CRITICAL ACTIONS NEEDED TO ADDRESS SHORTCOMINGS AND CHALLENGES IN IMPLEMENTING RESPONSIBILITIES: " DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION**

**RECOMMENDATION:**

The GAO recommends that the Secretary of Defense should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 5 years we identified.

The five (5) areas identified were: IT Leadership & Accountability, IT Strategic Planning, IT Workforce, IT Investment Management and Information Security.

**DoD RESPONSE:**

IT Leadership & Accountability. DoD concurs with the recommendation that the DoD CIO should provide input into “bureau” CIO performance evaluations. While the Department would require legislative relief to allow the DoD CIO to approve the selection of CIOs in the 3 Military Departments, it can and is in the process of drafting policy requiring that the designation of CIOs in other DoD Components be vetted with the DoD CIO. That policy would also allow the DoD CIO to provide input to those Components’ CIOs.

IT Strategic Planning. DoD partially concurs with the recommendation that DoD prepare an annual report on the progress in achieving the goals. It is the Department’s intent to include metrics in the next version of the DoD IRM Strategic Plan.

DoD also partially concurs with the recommendation that DoD issue policy requiring the CIO to benchmark agency processes against private and public sector performance. However, as part of the Department’s reform efforts, the IT and Business System Reform team when conducting research and analyses leverages industry and federal benchmarks. For example, the IT and Business System Reform Team leverages industry service level agreements, and industry and federal benchmarks when conducting research and analyses to build fact-based pricing and cost ranges for core enterprise technology agreements. For example, when conducting a review of the Military Health System’s IT Help Desks the IT & Business System Reform Group used efficiency benchmarks focused on total spend per employee as compared to similar private sector spend.

IT Workforce. DoD partially concurs with the recommendations associated with this area. The Department agrees with the first three recommendations associated with the IT workforce. The DoD CIO is the designated Functional Community Manager for 18 IT occupational series. As such, the Department has followed the procedures for workforce planning and assessment…

dictated by Section 115b of Title 10, United States Code, and as directed by the Under Secretary of Defense for Personnel and Readiness (USD P&R) in DoD Instruction 1400.25 Volume 250. These were annual processes until Section 115b was amended to a biennial requirement and then subsequently repealed. USD (P&R) is currently developing new guidance for functional community management. The DoD CIO will incorporate annual IT workforce reviews, as required, to dovetail with the overarching construct for the functional communities.

The Department partially concurs with the fourth finding, related to notification by the DoD CIO to the Secretary of Defense on the status of IT workforce matters. Prior to the cancellation of Section 115b and its reporting requirements, the Secretary of Defense submitted a comprehensive Strategic Human Capital Plan, including an appendix on the IT workforce developed by the DoD CIO, to Congress on an annual and then biennial basis. The most recent report was submitted in September 2016, providing an overview of the IT workforce. Since this reporting mechanism has been cancelled, the DoD CIO will identify a replacement process to continue Secretary of Defense awareness of IT workforce issues and initiatives.

IT Investment Mgmt. The DoD non-concurs with the GAO's assessment that the DoD policy does not require DoD CIOs to "certify that IT investments are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget." The DoD Financial Management Regulations (DoD 7000.14-R, Volume 2B, Chapter 18, Section 180102.G) requires a Statement of Compliance from each DoD Component submitting an electronic budget submission. Within the Statement, signed by the Component's CIO and CFO, Components are to indicate that the C!O certifies that information investments are adequately implementing incremental development, as defined in capital planning guidance issued by OMB.

The FY 2019 DoD certification of incremental development is documented in the DoD FY 2019 IT and Cybersecurity Activities Budget Overview (page 20). Reference: https://www.cape.osd.mil/content/SNAPIT/files/DoD FY2019 ITPresidentsBudgetReguestOver view°/o20-%20FINAL%20-%2020180309.pdf.

Information Security. DoD partially concurs with the recommendation, “Report annually to the agency head on the effectiveness of the agency information security program.” The DoD CIO currently provides an assessment of the Department’s information security program as part of the Department’s annual Federal Information Security Modernization Act (FISMA) report . This report is provided to the Secretary of Defense and the Deputy Secretary of Defense, and the requirement is documented in DoD Instruction 8500.01, “Cybersecurity.” In addition to the annual FISMA report, the DoD CIO provides an updated Cybersecurity Scorecard, which highlights critical elements of the Department’s cybersecurity posture, to the Deputy Secretary of Defense on a monthly basis. The Scorecard provides a more real-time view of the Department’s cybersecurity efforts and issues.

## Text of Appendix XX: Comments from the General Services Administration

Page 1

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U. S. Government Accountability Office (GAO) draft report entitled Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93).

In the draft report, GAO recommends that the Administrator of General Services ensure the agency’s information technology (IT) management policies address the role of the Chief Information Officer (CIO) for responsibilities in the following five key areas:

1. Strategic Planning;
2. Workforce;
3. Budgeting;
4. Investment Management; and
5. Information Security.

GSA is pleased that GAO found that GSA’s management policies address the CIO’s responsibilities in a sixth key area, IT area of leadership and accountability.

GSA partially concurs with GAO's findings outlined in this draft report. GSA recognizes that there are gaps in its formal policy directives. To address this, GSA has already begun to update or implement policies in order to fully address the role of the CIO, consistent with Federal law and guidance, in the key areas identified by GAO in the draft report.

However, GSA respectfully challenges the draft report's underlying premise that all individual CIO responsibilities must be codified into agency policy in order to assure efficacy of implementation. GSA requests that GAO consider that the GSA CIO implements responsibilities in these key areas, as demonstrated in the evidence provided below.

GSA has a long history of ensuring the CIO implements all responsibilities outlined in Federal law and Office of Management and Budget (OMB) guidance. Below are highlights of GSA IT business processes, artifacts, and operational activities that GSA actively leads, that align to the first four key areas noted above:

Page 2

1. Strategic Planning: GSA published and regularly updates both an IT Strategic Plan1 and a Data Center Optimization Initiative (DCOI) Strategic Plan in
2. compliance with existing OMB government wide guidance (M-16-19). In fact, GAO has previously identified GSA as an agency where effective Federal Information Technology Acquisition Reform Act practices have been demonstrated in the area of DCOI.
3. Workforce: GSA created a Competitive Development Program that is annually executed to assess staff skill sets and develop professional development opportunities. GSA Implemented an internal rotational program for continuing, on-the-job training of existing personnel. GSA implemented ‘‘Tech Talks” to share information and technology trends among different IT teams and across the agency. GSA also conducts an annual survey of training needs to identify and address vulnerabilities. In 2017, as a result of this survey, GSA identified a skill gap in the application of Agile principles and practices and trained over 87% of the staff in Agile application.
4. Budgeting: GSA serves as an early adopter of Technology Business Management (TBM) in the Federal space. GSA !T's TBM benchmarking capabilities will enable GSA to compare costs and

efficiencies against peer public sector organizations by geographic region and unit volumes.

5. Investment Management: GSA implemented a senior-executive-level governance board {sponsored by the Deputy Administrator and co-chaired by the CIO and Chief Financial Officer) to make technology investment decisions for the agency. To assist with benchmarking and investment planning, GSA engaged with research firms to compare the agency's percentage of total budget for IT spending versus industry averages, as well as for other key IT management benchmarks.

Finally, GSA disagrees with GAO's finding for key area 5, Information Security that GSA's IT Security policies "do not ensure all personnel are held accountable for complying with the agency-wide information security program." GSA has included a link to CID 2100.1K, GSA Information Technology (IT) Security Policy, June 30, 2017,2 which requires all employees and contractors to follow specific processes to ensure the safeguarding of GSA resources, and holds all personnel accountable for following and enforcing the IT security program. Chapter 1, paragraph 5, of this policy states:

6. Compliance and deviations. Compliance is mandatory immediately upon the signing of this Order. This IT Security Policy requires all GSA offices (SISO/R), Federal employees, contractors and other authorized users of GSA's IT resources, to comply with the security requirements outlined in this policy. This policy must be properly implemented, enforced, and followed to effectively protect GSA's IT resources and data. Appropriate disciplinary actions must be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of this GSA IT Security Policy may result in penalties under criminal and civil statutes.

Page 3

Because CIO 2100.1K ensures all personnel are held accountable for complying with the agency-wide information security program, GSA respectfully requests that this finding be changed to Fully Met.

If you have any additional questions or concerns, please contact me at (202) 501-0800 or Mr. Saul Japson, Acting Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

cc: Mr. David A. Powner,
Director, Information Technology Management Issues, GAO

## Text of Appendix XXI: Comments from the Small Business Administration

Page 1

Dear Mr. Powner:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled “Critical Actions Needed to Address Short Comings and Challenges in Implementing Responsibilities” GAO-18-93 (101056). The draft report analyzes the extent to which agencies have addressed the roles, responsibilities and duties of the Chief Information Officer (CIO) in accordance with Federal laws and guidance. SBA has reviewed the draft report and agrees with most of the recommendations but has concerns with the following findings:

- Evaluate IT investments according to risk (IT Dashboard): SBA firmly believes that its policies do require that each IT investment is reviewed utilizing a risk based evaluation. To classify the policy as not addressing the matter is inaccurate and should instead be reflected in the report as “Fully”.
- Report to the agency head or that official’s Deputy: The SBA CIO reports directly to the SBA Administrator and meets formally monthly to provide a status of all critical projects and activities. To classify the status as “Not at All” is inaccurate and should instead be reflected in the report as “Fully”.
- Review and approve IT budget requests: SBA established a policy requiring all IT acquisitions greater than $50,000 be reviewed and approved by the CIO prior to a solicitation being released. To classify the status as “Not at All” is inaccurate and should instead be reflected in the report as “Fully” addressed.
- Improve the management of the agency’s IT portfolio through portfolio review (PortfolioStat): SBA uses several governance tools to review its IT portfolio. The SBA CIO meets quarterly with OMB for PortfolioStats. The CIO also conducts TechStats and Deep Dive reviews on any IT investment that is having challenges.

To classify the status as “Not at All” is inaccurate and should instead be reflected in the report as “Fully” addressed.

- Evaluate IT investments according to risk (IT Dashboard CIO ratings): The SBA CIO reviews all major IT investments on a monthly basis to evaluate IT investments for the OMB IT Dashboard CIO ratings. To classify the status as “Not at All” is inaccurate and should instead be reflected in the report as “Fully”.

Page 2

- Review high-risk IT investments using TechStat sessions: According to the response we received in January from GAO the status would be changed from “Not addressed to Partially Addressed”. The draft report does not reflect this agreed upon adjustment.
- Maintain an inventory of data centers: SBA maintains an inventory of our data centers and can provide this information to GAO. To classify the status as “Not at All” is inaccurate and should instead be reflected in the report as “Fully” addressed.
- Maintain a strategy to consolidate and optimize data centers: SBA has a strategy regarding the consolidation and optimization of its data centers. The document is located on the SBA website (click here) in accordance to the OMB requirement that SBA maintain and update its data center optimization strategy. To classify the status as “Not at All” is inaccurate and should instead be reflected in the report as “Fully”.

Thank you for the opportunity to comment on this draft report and for taking SBA’s views into consideration prior to publishing the final report.

Sincerely,

Maria Roat
Chief Information Officer

## Text of Appendix XXII: Comments from the Nuclear Regulatory Commission

Page 1

Dear Mr. Powner:

Thank you for providing the U.S. Nuclear Regulatory Commission (NRG) with the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93." The NRG has reviewed the draft report and is in general agreement with its findings. However, the NRG is not in agreement with GAO's recommendations for the NRG, as explained in the enclosure.

If you have any questions about the NRC's response, please contact John Jolicoeur by telephone at (301) 415-1642 or by e-mail at John.Jolicoeur@nrc.gov.

Sincerely,

Victor M. McCree
Executive Director for Operations

Enclosure: NRG Comments on GAO-18-93

Page 2

**Comments on the U.S. Government Accountability Office's Draft Report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93"**

The U.S. Nuclear Regulatory Commission (NRG) reviewed the U.S. Government Accountability Office's (GAO's) draft report, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcoming and Challenges in Implementing Responsibilities GAO-18-93," and has the comments discussed in this paper.

In Table 24, "Extent to Which Nuclear Regulatory Commission Policies Address the Role of its Chief Information Officer (CIO)," GAO rated the NRG against 35 key responsibilities in 6 areas:

(1) leadership and accountability, (2) strategic planning, (3) workforce, (4) budgeting,

(5) investment management, and (6) information security. The NRG is in general agreement with the GAO findings. However, the NRG is not in agreement with the GAO recommendations on information technology

(IT) leadership and accountability, workforce, and investment management. The agency's comments for these areas are provided below.

**IT Leadership and Accountability**

- Report directly to the agency head or that official's deputy. The NRG is fully compliant with this requirement. NRG-specific organizational legislation (Reorganization Plan No. 1 of 1980) assigns the agency's "administrative functions" to the Chairman and then requires the Chairman to delegate them to the Executive Director for Operations. The NRC's CIO reports directly to the Executive Director for Operations, who serves as the Chief Operating Officer (COO). The CIO also has direct access to the Chairman. This is consistent with the requirements laid out in Element Q1 of the Federal IT Acquisition Reform Act (FITARA) Common Baseline, which states the following:
  QI. CIO reports to agency head (or deputy/COO). As required by the Clinger Cohen Act and left in place by FITARA, the CIO "shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter."

This provision remains unchanged, though certain agencies have since implemented legislation under which the CIO and other management officials report to a COO, Undersecretary for Management, Assistant Secretary for Administration, or similar management executive; in these cases, to remain consistent with the Clinger Cohen requirement as left unchanged by FITARA, the CIO shall have direct access to the agency head (i.e., the Secretary, or Deputy Secretary serving on the Secretary's behalf) regarding programs that include information technology.

**IT Workforce**

- Assess annually the requirements established for agency personnel regarding IT management knowledge and skills. The NRC believes it is partially compliant with this requirement. Page 23 of the NRC's Capital Planning and Investment Control Policy and Overview, Version 2.0, issued October 2016 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML16272A383), includes the following among the CIO's responsibilities:

Enclosure

Jointly with the CHCO, develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership positions) and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

The NRC also recently reissued Management Directive (MD) 12. 5, “NRC Cybersecurity Program,” dated November 2, 2017 (ADAMS Accession No. ML172788085), to specifically define these CIO responsibilities.

- Assess annually the extent to which agency personnel meet IT management knowledge and skill requirements. The NRC believes it is partially compliant with this requirement. Page 23 of the NRC’s Capital Planning and Investment Control Policy and Overview (ADAMS Accession No. ML16272A383) states the following:
  Jointly with the CHCO, develop a set of competency requirements for IT and IT acquisition staff (including IT and IT acquisition leadership positions) and develop and maintain a current workforce planning process to ensure the agency can anticipate and respond to changing mission requirements, maintain workforce skills in a rapidly developing IT environment, and recruit and retain the IT talent needed to accomplish the mission.

The NRC also recently reissued MD 12.5 (ADAMS Accession No. ML17278B085) to specifically define these CIO responsibilities.

- Annually develop strategies for hiring and training to rectify any knowledge and skill deficiencies. The NRC believes it is partially compliant with this requirement. Part 111, Section I, of MD 10.1, “Recruitment, Appointments, and Merit Staffing,” dated May 5, 2015 (ADAMS Accession No. ML14092A397), and Part 111, Section E, of MD 10.77, “Employee Development and Training,” dated January 4, 2016 (ADAMS Accession No. ML15341A156), require all NRC Office Directors to work with the Chief Human Capital Officer (CHCO) annually to build an annual staffing plan and a prioritized list of training for their staff. The CIO is an Office Director and is therefore required to work with the CHCO annually to build an annual staffing plan and a prioritized list of training for OCIO staff.

In addition, the CIO participates in the NRC's strategic workforce planning, as evident in the NRC's Strategic Workforce Plan, dated February 4, 2016 (ADAMS Accession No. ML16145A376). The strategic workforce plan ensures that the NRC is positioned to have the right number of people with the right competencies at the right time.

**IT Investment Management**

- Maintain strategy to consolidate and optimize data centers. The NRC is fully compliant with this requirement. The NRC maintains and posts the Data Center Optimization Initiative Strategic Plan on the NRC public Web site located at https://www.nrc.gov/public-involve/open/digital-government.html#data. The agency has also provided the CIO certification memorandum signed by the NRC CIO to the Federal CIO and has posted it on the NRC public Web site located at https://www.nrc.gov/public-involve/open/digital- government/dcoi-strategic-plan-cio-certification-20170414.pdf.

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

Page 1

Dear Mr. Walsh:

Thank you for the opportunity to comment on the U.S. Government Accountability Office (GAO) draft report entitled, Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93). The Department of Housing and Urban Development reviewed the draft report and has no comments.

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), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.gov).

Sincerely,

Chad Cowan, Jr.
Acting Chief Information Officer

Page 2

cc:

Kevin R. Cooke, Jr., Principal Deputy Chief Information Officer, Q

Janice Ausby, Deputy CIO for Business and IT Resource Management, QRM Tracy Bigesby, Deputy Chief Information Security Officer, OCIO, QS

Felicia Gaither, Supervisory Management Analyst, Strategic Planning Staff, OCIO, QMS Jeffrey Cohen, Supervisory Budget Analyst, Portfolio Management Branch, OCIO, QRMM Wynee Watts-Mitchell, Director, Audit Compliance Branch, OCIO, QMAC

Juanita Toatley, IT Specialist, Audit Compliance Branch, OCIO, QMAC

Helen McBride, Senior Advisor to the Principal Deputy Chief Information Officer, Q Gloria Holder, Jr., Management Analyst, Administrative Services Branch, OCIO, QMAS Larry McGhee, Director, Audit Liaison Division, OCFO, FMA

## Text of Appendix XXIV: Comments from the Environmental Protection Agency

Page 1

**MEMORANDUM**

SUBJECT: EPA’s Response to GAO-18-93 Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities 101056).

FROM: Steven Fine, Ph.D.
Acting Assistant Administrator and Acting Chief Information Officer

TO: Kevin Walsh, Assistant Director, GAO

The Office of Environmental Information (OEI)) reviewed the Draft Report, GAO-18-93, Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (101056).

The purpose of this memorandum is to provide EPA's response to the report.

In the Draft Report, GAO recommends that "The Administrator of the Environmental Protection Agency should ensure that the department's IT management policies address the role of the CIO for key responsibilities in the 6 areas [GAO] identified".

**Response:**

EPA agrees in principle that CIO authorities should be adequately documented in appropriate policies. This audit documents a large number of CIO authorities that are not yet captured in policy documents. Some of these are items that lack policy or other supporting process or documentation; others have supporting processes in place and simply require a policy statement to formalize the authority. In addition, some require assessment as to whether we are positioned, either from a resource or process ownership perspective, to implement a policy.

CIO staff, working with Agency senior leaders, set an annual IT policy agenda documenting which policy items will be worked that year. This assures that we devote our resources to the most important policy matters. I will work with my policy staff to determine which of the items

listed in this report are (a) already on the FY18 policy agenda (e.g., we are planning to draft a FITARA implementation policy that will cover some of the items cited in this report, including certification of incremental development) and (b) which should be included on the FY19 policy agenda, given the full environment of IT policy priorities for the agency.

cc: Mark T. Howard, OCFO Bob Trent, OCFO
Patricia Randolph Williams, OEI Elena Larsen, OEI
Patrick Grimm, OEI Juanita Standifer, OEI

# Text of Appendix XXV: Comments from the U.S. Agency for International Development

Page 1

Dear Mr. Pawner:

I am pleased to provide the formal response of the United States Agency for International Development (USAID) to the draft report of the U.S. Government Accountability Office (GAO) entitled “FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities” (GAO-18-93). USAID is committed to full compliance with the requirements of the Federal Information Security Modernization Act and the Federal Information Technology Acquisition Refo1m Act, and we view the statutory mandates as integral components of our risk management framework. We have made significant improvements in our information technology (IT) policies and processes since the GAO completed its survey, and our response highlights our ongoing efforts to institutionalize these processes as formal published policy.

I am transmitting this letter and the enclosed USAID comments for incorporation as an appendix to the GAO’s final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

Angelique M. Crumbly
Acting Assistant Administrator
Bureau for Management

Enclosure: a/s

Page 2

**COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT – FEDERAL CHIEF INFORMATION OFFICERS: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities (GAO-18-93)**

USAID has three comments on Draft Report 18-93 prepared by the Government Accountability Office (GAO):

1. USAID believes that many of the deficiencies identified in the Draft Repo1i are better characterized as gaps in documentation, as the Agency’s Chief Information Officer (CIO) is already performing the key responsibilities listed. While USAID might not yet have published policies that fully describe how the Agency’s policies to manage information technology (IT) address the role of the CIO in all areas, this does not mean the USAID CIO lacks, or does not perform these key functions. In fact, with the exception of those items that are not applicable (USAID does not have individual Bureau- level CIOs or non-cloud data centers), USAID’s CIO is performing nearly all of the key responsibilities outlined in GAO Draft Report 18-93. For example, the USAID CIO regularly reviews the Agency IT Portfolio through PortfolioStat with the Office of Management and Budget (OMB); regularly evaluates IT programs according to risk, through an IT Dashboard; and certifies that IT investments are adequately using incremental development. These are all areas for which official Agency IT management policies might have been missing at the time of the audit, but for which we are now revising a chapter of our Automated Directive System (ADS), USAID’s official policy manual.

2. USAID would like to bring to GAO’s attention the actions we have completed and those that are currently underway to address the identified gaps in USAID policy. The table below lists each CIO responsibility identified by GAO, and captures USAID’s response, or action taken. Overall, we are now fulfilling seven of the responsibilities that GAO identified as unmet. Additionally, the Agency will fulfill eight areas in the coming months, with the publication of USAID’s new policy on implementing the Federal Information Technology Acquisition Reform Act (FITARA). Finally, we are currently addressing in policy updates, six of the responsibilities that GAO identified as not fully met.

3. USAID agrees that additional guidance from OMB to define CIOs' authorities clearly will assist in our efforts to consolidate our IT planning, budgeting, and programming further.

This report has one recommendation for USAID, as shown on page 41 of the draft report:

**Recommendation 1:**

The Administrator of the U.S. Agency for International Development should ensure the Agency's management IT policies address the role of the CIO for key responsibilities in the 6 areas we identified.

In accordance with the GAO's recommendation the Agency' s Transformation plan, approved by the Office of Management and Budget, and which we will notify to Congress in early June, will propose making the CIO a direct rep01i to the Administrator, while the institutional home for the CIO's office will remain the Management Bureau. The Bureau for Management will also take action, in coordination with…

Page 3

the Agency Transformation, to ensure the Agency's IT management policies document the role and responsibilities of the CIO in the six areas GAO identified. We plan to publish the revised policy, ADS Chapter 509, by the beginning of June as well. This will institutionalize the functions of the CIO in a clear way.

Attached, please find a detailed table that outlines what USAID has already done to account for GAO's recommendations, and specifies the areas in which we will be taking actions in the near future.

## 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 (https://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 https://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, https://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 https://www.gao.gov.

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

Contact:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

## Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

## Public Affairs

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

## Strategic Planning and External Liaison

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