



April 2015

FEDERAL CHIEF INFORMATION OFFICERS

Reporting to OMB
Can Be Improved by
Further Streamlining
and Better Focusing
on Priorities

GAO Highlights

Highlights of [GAO-15-106](#), a report to congressional requesters

Why GAO Did This Study

Federal agencies annually invest over \$80 billion on IT. As part of overseeing this spending, OMB directs federal CIOs to report on their management of IT in such areas as capital planning and investment management, security, and strategic planning.

GAO was asked to review the usefulness of such CIO reporting requirements. Its objectives were to (1) identify the current IT reporting requirements that agency CIOs are to address for OMB, (2) evaluate the extent to which OMB and agency CIOs use the required information to manage IT, including CIOs' views on the utility of the requirements, and (3) assess any OMB efforts to streamline this reporting. To do so, GAO analyzed OMB memorandums and other guidance to develop a list of CIO requirements and surveyed 24 major agency CIOs on how they used the required information to manage IT. Further, it analyzed OMB documentation and interviewed officials to identify plans to streamline reporting.

What GAO Recommends

GAO is recommending that OMB, in collaboration with CIOs, ensure a common understanding of priority IT reforms and their reporting requirements and address proposed reporting improvements and challenges. OMB neither agreed nor disagreed with GAO's recommendations, citing concerns with, among other things, GAO's survey methodology, stating it did not fully support the report's findings and recommendations. GAO believes these concerns are largely unfounded and that its recommendations are still valid.

View [GAO-15-106](#). For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

April 2015

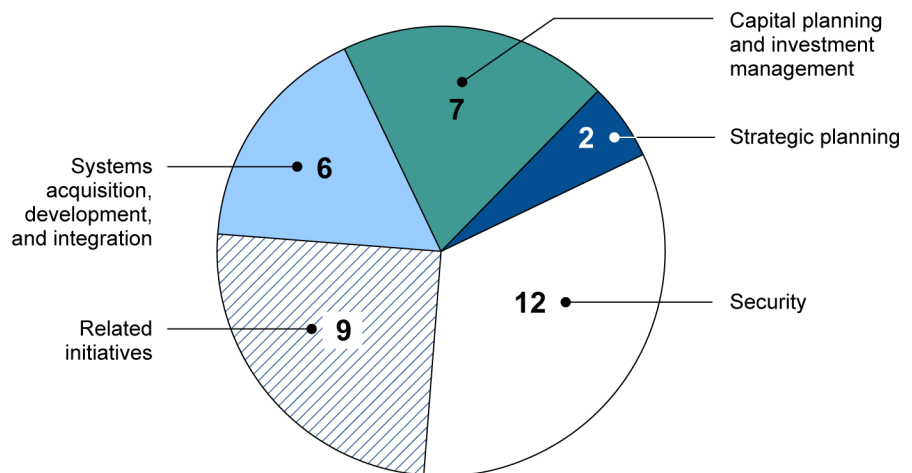
FEDERAL CHIEF INFORMATION OFFICERS

Reporting to OMB Can Be Improved by Further Streamlining and Better Focusing on Priorities

What GAO Found

The Office of Management and Budget (OMB) directs agency chief information officers (CIO) to respond to 36 information technology (IT) management reporting requirements, largely on a quarterly or annual basis, that address several areas key to effective IT management (see figure).

Number of Requirements per Key IT Management Area



Source: GAO analysis. | GAO-15-106

OMB uses the information reported by CIOs to help it oversee the federal government's use of IT, including implementation of OMB's IT reform initiatives such as consolidating data centers and eliminating duplication. A majority of 24 CIOs surveyed that responded reported that 24 of the 36 reporting requirements help only to some to no extent in managing IT and that meeting them took significant effort and cost approximately \$150 million to \$308 million annually. A number of CIOs further noted that these requirements were not always helpful because, among other things, addressing them did not support agency priorities. Nonetheless, GAO has previously emphasized the importance of OMB's reforms and their associated reporting requirements to improving federal IT management and producing savings. Thus it is concerning that CIOs do not always see value in reporting information essential to these reforms. Establishing a common understanding between OMB and CIOs on the priority of these initiatives and their related reporting requirements will help ensure their success.

OMB has taken steps to streamline CIO reporting requirements, such as changing reporting formats from narratives to performance data. Nonetheless, OMB's efforts do not address challenges identified by CIOs, such as tracking all current requirements and having to use multiple online tools to report information. This is partly because OMB has not solicited feedback in these areas, due to its focus on streamlining reporting in other areas. By not addressing these challenges, OMB is missing opportunities to help CIOs improve the requirements reporting process and its use of information collected to effectively manage and oversee federal IT.

Contents

Letter		1
	Background	2
	Agency CIOs Are to Address 36 IT Management Reporting Requirements for OMB	11
	Although OMB Uses Required Information, CIOs Reported That the Majority of Reporting Requirements Are Not Useful for Managing IT and Identified Areas for Improvement	18
	OMB Has Initiated Efforts to Streamline Reporting, but They Do Not Address Challenges Reported by CIOs	30
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments and Our Evaluation	36
Appendix I	Objectives, Scope, and Methodology	45
Appendix II	Chief Information Officer IT Management Reporting Requirements	49
Appendix III	Survey of Federal Agency Chief Information Officers	51
Appendix IV	Comments from the Office of Management and Budget	58
Appendix V	GAO Contact and Staff Acknowledgments	63
Tables		
	Table 1: CIO Reporting Requirements with Description, Reporting Frequency, and Mechanism, as of March 2014	12
	Table 2: Extent to Which Addressing the 36 Reporting Requirements Is Useful to Managing IT	21
	Table 3: Reporting Requirements by Chief Information Officer-Reported Usefulness in Assisting in Managing Agency IT, Level of Effort, and Estimated Total Annual Cost	24
	Table 4: Agency Chief Information Officer (CIO) Proposed Changes to Reporting Requirements	26

Table 5: Chief Information Officer Reporting Requirements, including Source and Year Established	49
---	----

Figure	Figure 1: Number of Requirements per Key IT Management Area	16
--------	---	----

Abbreviations	
CIO	Chief Information Officer
CFO	Chief Financial Officer
IT	information technology
OMB	Office of Management and Budget

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



April 2, 2015

The Honorable Ron Johnson
Chairman
The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Michael T. McCaul
Chairman
Committee on Homeland Security
House of Representatives

The federal government annually invests more than \$80 billion on information technology (IT). As part of budgeting for and overseeing this spending, the Office of Management and Budget (OMB) directs federal agency chief information officers (CIO) to report on their management of IT in such areas as capital planning and investment management, security, and strategic planning. The goal of these reports is to, among other things, optimize investment of IT funds and address long-standing federal agency IT management problems.

You asked that we review the usefulness of such CIO reporting requirements. Our objectives were to (1) identify the current IT reporting requirements that agency CIOs are to address for OMB; (2) evaluate the extent to which OMB and agency CIOs use the required information to manage IT, including CIOs' views on the utility of the requirements; and (3) assess any OMB efforts to streamline this reporting.

To address these objectives, we obtained and analyzed OMB memorandums and other guidance to develop a list of CIO requirements that were regular, repeating, or one-time requests. Since there could be several requirements for information in multiple OMB memorandums for one initiative, we grouped the requirements to report information together by initiative and the frequency of reporting rather than list each as its own separate requirement. In doing this, we had all agencies in our review

(the 24 Chief Financial Officer (CFO) Act agencies¹) and OMB review our list and provide feedback to help ensure the list was complete and accurate. Requirements related to activities such as information collection and control of paperwork; records management; privacy and compliance with the Privacy Act; and information disclosure and compliance with the Freedom of Information Act were not included because these activities are not directly related to IT management responsibilities. In addition, we obtained and analyzed OMB documentation and interviewed OMB officials to determine the extent to which they use the information reported by agencies to further the goal of improving the management of federal IT; we also conducted a web-based survey of the 24 CFO Act agencies to obtain information on how they used the required information to manage IT. All 24 agencies completed the survey, although not all survey respondents answered every question. Further, we analyzed OMB and Federal CIO Council² documentation and interviewed officials to assess current and future plans to streamline CIO reporting and the extent to which these efforts assist OMB's goal of reducing CIO reporting burden.

We conducted this performance audit from December 2013 to April 2015 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. Details on our objectives, scope, and methodology are in appendix I.

Background

Over the years, Congress has enacted various laws in an attempt to improve the government's management of its IT resources. In doing so, it

¹The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Office of Personnel Management, Small Business Administration, Social Security Administration, U.S. Agency for International Development, and the U.S. Nuclear Regulatory Commission.

²The Federal CIO Council is the principal interagency forum to improve agency practices in such matters as the design, modernization, use, sharing, and performance of agency information resources.

has provided OMB with broad IT management and oversight responsibilities and given agencies a wide range of IT-related responsibilities.³ With regard to CIO responsibilities relative to IT management, we have previously identified major areas that are either statutory requirements or are critical to effective IT management.⁴ These areas include:

- **IT strategic planning:** Plans for, among other things, using IT to help agencies improve the productivity, efficiency, and effectiveness of their business processes with the overall goal of achieving and supporting agency missions.
- **Capital planning and investment management:** The process of selecting, controlling, and evaluating IT investments to produce business value, reduce investment-related risks, and increase accountability and transparency in the investment decision-making process.
- **IT security:** Establishment of a risk-based program that ensures agency-wide compliance with requirements to protect information and systems, including implementing requisite controls that prevent, limit, or detect access to computer networks, systems, or information.
- **Systems acquisitions, development, and integration:** Obtain the skilled staff, disciplined processes, and tools necessary to develop and acquire IT system capabilities on time and within budget, including ensuring such capabilities interoperate as intended with existing (legacy) systems.
- **E-government initiatives:** A wide range of activities across the federal government involving the use of the Internet and other emerging technologies to improve public access to government information and services.

³The sources of the major federal IT management requirements are the Clinger-Cohen Act of 1996 (40 U.S.C. § 11101, et seq.), the Paperwork Reduction Act of 1995 (44 U.S.C. § 3501, et seq.), the Federal Information Security Management Act of 2002 (44 U.S.C. § 3541, et seq.), and the E-Government Act of 2002 (Pub. L. No. 107-347, Dec. 17, 2002). As of December 18, 2014, the Federal Information Security Management Act of 2002 was largely superseded by the Federal Information Security Modernization Act of 2014 (44 U.S.C. § 3551, et seq.; Pub. L. No. 113-283, Dec. 18, 2014).

⁴GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, [GAO-04-823](#) (Washington, D.C.: July 21, 2004). In this report, we identified a total of 13 major areas of responsibility, including 7 in IT management and 6 in information management.

To carry out their responsibilities, OMB (including its Office of E-Government and Information Technology, headed by the Federal CIO) issues directives to the agencies such as circulars, memorandums, and reporting instructions; these directives contain requirements for agency CIOs to, among other things, report on their IT activities. For example, OMB Circular A-11 requires agencies to provide information related to their IT investments, including agency exhibit 53s and capital asset plans and business cases (called exhibit 300s). In addition, in December 2011, OMB issued a memorandum that outlines the Federal Risk and Authorization Management Program⁵ guidance for agency adoption and use of cloud services.

For each reporting requirement, OMB typically identifies how agencies are to transmit the information. In particular, OMB operates and utilizes the following web-based systems that the agencies are to use to transmit their information:

- **CyberScope:** Standardizes manual and automated data inputs for reporting on Federal Information Security Management Act⁶ compliance and agency privacy programs.
- **Integrated Data Collection:** Allows reporting of structured information, including agency progress in meeting IT strategic goals, objectives and metrics, as well as cost savings and avoidances resulting from IT management actions. These data include information previously reported by agencies as well as data which agencies shall report on every 3 months. Updates are to be made on the last day of February, May, August, and November of subsequent fiscal years.

⁵The Federal Risk and Authorization Management Program—commonly referred to by OMB and the agencies as FedRAMP—is a government-wide program to provide joint authorizations and continuous security monitoring services for all federal agencies. See OMB, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

⁶As noted above, the 2002 Federal Information Security Management Act has been largely superseded by the 2014 Federal Information Security Modernization Act. While the 2014 law generally continues the same agency information security requirements, it included some changes to agency reporting requirements. These changes will likely be reflected in future OMB and Department of Homeland Security guidance, but were not reflected in the reporting requirements that were the subject of this review. Additionally, although OMB has incorporated agency reporting on privacy-related issues into annual Federal Information Security Management Act reporting, we have not included privacy since it was considered outside the scope of our work. See app. I for more details.

-
- **MAX Portal:** Utilized by federal agencies to enter data and upload documentation related to a variety of reporting activities, including data required for the President's Budget and Mid-Session review, and federal IT investment information.
 - **Federal IT Dashboard:** Allows federal agencies to upload cost, schedule, and performance data on agency major IT investments.⁷

In addition to the reporting system mechanisms listed above, OMB occasionally requires agencies to provide information by e-mail (usually for ad hoc requests) or directs agencies to post information on their websites. For example, with regard to an OMB reporting requirement on open data policies, OMB directs the agencies to post this information on their websites.

To help CIOs prioritize their various roles and responsibilities, OMB has directed CIOs to focus their efforts on the following⁸:

- **Governance.** CIOs should have responsibility over the entire IT portfolio for the agency, including driving the investment review process for IT investments, working with CFOs and Chief Acquisition Officers to ensure IT portfolio analysis is part of the yearly budget process, and leading TechStat sessions.⁹
- **Commodity IT.** CIOs should focus on eliminating duplication in commodity IT services (e.g., data centers, e-mail, and web infrastructure) and rationalize their agency's IT investments, including using shared services as a provider instead of standing up separate services.

⁷The IT Dashboard is a public website that is to provide transparency and oversight of agencies' IT investments by displaying federal agencies' cost, schedule, and performance data for over 700 major federal IT investments at 27 federal agencies, accounting for \$38.7 billion of those agencies' planned \$82 billion budget for fiscal year 2014. OMB defines a major IT investment as one needing special management attention due to, among other things, its importance to carrying out an agency's mission or high development, operating, or maintenance costs (e.g., more than \$500,000).

⁸OMB, *Chief Information Officer Authorities*, M-11-29 (Washington, D.C.: Aug. 8, 2011).

⁹In January 2010, OMB began conducting TechStats, which are face-to-face, evidence-based reviews of an at-risk IT investment. Subsequently, as part of the Federal CIO's 25-point IT Reform Plan, OMB empowered agency CIOs to hold their own TechStat sessions within their respective agencies and required agencies to hold at least one TechStat session by March 2011, and one bureau-led TechStat review by June 2012. In August 2011, OMB M-11-29 required agency CIOs to continue holding TechStat sessions.

-
- **Program management.** CIOs should improve the overall management of federal IT projects by identifying, recruiting, and hiring top IT program management talent and be accountable for the performance of agency IT program managers.
 - **Information security.** CIOs should have the authority and primary responsibility for implementing an agency-wide information security program, including having continuous monitoring and standardized risk assessment processes.

In addition, OMB has implemented a series of initiatives—commonly referred to by the agency as IT reforms—to, among other things, improve the oversight of underperforming investments, more effectively manage IT, and address duplicative investments. The initiatives include the following:

- **TechStat reviews.** In January 2010, the Federal CIO began leading TechStat sessions—face-to-face meetings to terminate or turn around IT investments that are failing or are not producing results. These meetings involve OMB and agency leadership and are intended to increase accountability and transparency and improve performance. Subsequently, OMB empowered agency CIOs to hold their own TechStat sessions within their respective agencies. OMB has reported that these efforts to improve management and oversight of IT investments have resulted in almost \$4 billion in savings.
- **Federal Data Center Consolidation Initiative.** Concerned about the growing number of federal data centers, the Federal CIO (in February 2010) established the Federal Data Center Consolidation Initiative. The initiative’s four high-level goals were to promote the use of “green IT”¹⁰ by reducing the overall energy and real estate needs of government data centers; reduce the cost of data center hardware, software, and operations; increase the overall IT security posture of the government; and shift IT investments to more efficient computing platforms and technologies. OMB estimates that the initiative has the potential to provide about \$3 billion in savings by the end of 2015.
- **PortfolioStat.** In order to eliminate duplication, move to shared services, and improve portfolio management processes, OMB (in

¹⁰“Green IT” refers to environmentally sound computing practices that can include a variety of efforts, such as using energy-efficient data centers, purchasing computers that meet certain environmental standards, and recycling obsolete electronics.

March 2012) launched its PortfolioStat initiative. It required agencies to conduct annual agency-wide IT portfolio reviews to, among other things, reduce commodity IT¹¹ spending and demonstrate how IT investments align with agency mission and business functions.¹² PortfolioStat is designed to assist agencies in (1) assessing the current maturity of their IT investment management process, (2) making decisions on eliminating duplicative investments, and (3) moving to shared solutions in order to maximize the return on IT investments across the portfolio. OMB estimates that the PortfolioStat effort has the potential to save \$2.5 billion from fiscal year 2013 through fiscal year 2015 by, for example, consolidating duplicative systems.¹³

Given the importance of these initiatives, OMB has established reporting requirements to, among other things, track the status of agencies' implementation of these efforts. In addition, Congress recently incorporated key aspects of a number of these reforms into law.¹⁴

Our extensive experience at federal agencies and in particular, our recent reports on TechStat,¹⁵ data center consolidation,¹⁶ and PortfolioStat,¹⁷

¹¹According to OMB, commodity IT includes services, such as enterprise IT systems (e-mail; identity and access management; IT security; web hosting, infrastructure, and content; and collaboration tools); IT infrastructure (desktop systems, mainframes and servers, mobile devices, and telecommunications); and business systems (financial management, grants-related federal financial assistance, grants-related transfer to state and local governments, and human resources management systems).

¹²OMB, *Implementing PortfolioStat*, M-12-10 (Washington, D.C.: Mar. 30, 2012).

¹³We subsequently reviewed this estimate and determined that it was underestimated because it, among other things, did not include estimates from the Departments of Defense and Justice. For the results of this review, see GAO, *Information Technology: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings*, [GAO-14-65](#) (Washington, D.C.: Nov. 6, 2013). We also discuss these results later in this report.

¹⁴See the federal information technology acquisition reform provisions (commonly referred to as the Federal Information Technology Acquisition Reform Act or FITARA) of the 2015 Defense Authorization Act. Sections 831 – 837, The Carl Levin & Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291 (Dec. 19, 2014).

¹⁵GAO, *Information Technology: Additional Executive Review Sessions Needed to Address Troubled Projects*, [GAO-13-524](#) (Washington, D.C.: June 13, 2013).

¹⁶GAO, *Data Center Consolidations: Reporting Can Be Improved to Reflect Substantial Planned Savings*, [GAO-14-713](#) (Washington, D.C.: Sept. 25, 2014).

have shown that these reforms and the required information agencies are to report on to OMB as part of these efforts offer important opportunities to improve the efficiency and effectiveness of federal agency programs and operations, including producing financial savings. The reports also included recommendations to OMB to improve agency reporting on key initiatives; the recommendations highlighted the importance of OMB's reporting requirements and the need for federal agencies to provide current and accurate information about the status of these initiatives. They also highlighted that the requirements are a critical component to ensuring OMB's effective management and oversight of the initiatives.

Together, the responsibilities discussed above require CIOs to be key leaders in managing IT in a coordinated fashion in order to improve the efficiency and effectiveness of programs and operations.

OMB Has Periodically Changed CIO Requirements to Address Changes in Federal IT Management

Over the last several years, OMB has made changes to CIO reporting requirements to address, among other things, changes in federal IT management. Such changes included modifying how requirements are reported, updating what information is requested as part of existing requirements, and establishing new requirements. For example, in March 2013, OMB issued a memorandum¹⁷ which, among other things, established the Integrated Data Collection, which was a new way for agencies to submit information relating to IT reform initiatives such as PortfolioStat and data center consolidation.

Further, in July 2013, OMB requested in its fiscal year 2015 budgetary exhibits 53 and 300 guidance that agencies provide additional documentation on investments.¹⁹ For example, OMB requested that agencies provide any operational analyses²⁰ performed on existing (legacy) investments in operations and maintenance. It also requested

¹⁷ [GAO-14-65](#).

¹⁸ OMB, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, M-13-09 (Washington, D.C.: Mar. 27, 2013).

¹⁹ OMB, *Fiscal Year 2015 Guidance on Exhibits 53 and 300 – Information Technology and E-Government* (Washington, D.C.: July 1, 2013).

²⁰ Operational analyses are a key performance evaluation and oversight mechanism required by OMB to ensure investments in operations and maintenance are continuing to meet agency needs. Per OMB guidance, agencies are to annually perform these analyses on their investments that are in operations and maintenance.

agencies provide information on investments that are to be reduced or eliminated as the result of new investments.

Moreover, in May 2014, OMB issued updated instructions for the Integrated Data Collection, aimed at improving the quality of data, which changed the format and information reported for several requirements, as well as adding a new reporting requirement on progress in using standard customer value methodologies to evaluate agencies' highest impact IT services.²¹

Prior GAO Reports Have Recommended Improvements to IT Reform Initiatives and Associated Reporting

During the past several years, we have reported on a variety of issues related to CIOs' roles and responsibilities and OMB's management and reporting of information obtained through federal agency reporting requirements.²² For example, in September 2011, we reported on the roles and responsibilities of agency CIOs.²³ Specifically, we found that although most CIOs are responsible for major areas of IT (e.g., capital planning, IT strategic planning, and e-government initiatives), they are less frequently responsible for other information management areas (e.g., records management and privacy) that, despite being required by law, are considered not critical to effective IT management. We recommended that OMB update its guidance to establish measures of accountability for ensuring that CIOs' responsibilities are fully implemented and require agencies to establish internal processes for documenting lessons learned. OMB agreed with our recommendations and stated that it had taken actions that it believed addressed the recommendations; we are currently in the process of validating whether these actions fully address our recommendations.

²¹OMB, *Fiscal Year 2014 PortfolioStat*, M-14-08 (Washington, D.C.: May 7, 2014).

²²GAO, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation*, [GAO-06-831](#) (Washington, DC: Aug. 14, 2006); *Information Technology: Management and Oversight of Projects Totaling Billions of Dollars Need Attention*, [GAO-09-624T](#) (Washington, D.C.: Apr. 28, 2009); *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, [GAO-11-634](#) (Washington, D.C.: Sept. 15, 2011); *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal*, [GAO-13-378](#) (Washington, D.C.: Apr. 23, 2013); *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to be More Accurate and Reliable*, [GAO-14-64](#) (Washington, D.C.: Dec. 12, 2013); and [GAO-14-65](#).

²³[GAO-11-634](#).

In addition, in November 2013, we found that of the 26 major federal agencies that were required to participate in the PortfolioStat initiative—an annual agency-wide portfolio review—only 1 agency addressed all of the key requirements.²⁴ We also determined that OMB’s estimate of \$2.5 billion in savings from PortfolioStat was understated because it, among other things, did not include estimates from the Departments of Defense and Justice. Our analysis, which included these estimates, showed that agencies were reporting at least \$5.8 billion in potential savings. Further, not all agencies provided sufficient support for their estimated potential savings on consolidation initiatives. We recommended that OMB and the agencies improve their PortfolioStat implementation, and the parties agreed in large part with our recommendations; we are currently following up to assess their progress in doing so.

Further, in December 2013, we reported that although the accuracy of ratings on the Federal IT Dashboard had improved, they were inconsistent among the agencies we reviewed.²⁵ In addition, we found that the public version of the Dashboard was not updated for 15 of the past 24 months, and so was not available as a tool for investment oversight and decision making. We recommended that OMB make Dashboard information available independent of the budget process and agencies appropriately categorize IT investments and address identified weaknesses. OMB neither agreed nor disagreed with our recommendations. Nonetheless, we have ongoing work to assess the extent to which OMB and agencies have implemented the recommendations.

More recently, in September 2014, we reported on federal agencies’ progress in reducing duplication and overlap in their IT data centers (defined as data storage facilities).²⁶ We had previously reported on weaknesses in agencies’ efforts and OMB’s oversight. In our most recent report, we determined that while agencies’ reported cost savings and avoidances through fiscal year 2015 totals approximately \$3.3 billion—or about \$300 million higher than OMB’s original \$3 billion goal—planned savings may be higher. Specifically, six agencies reported little or no cost

²⁴ [GAO-14-65](#).

²⁵ [GAO-14-64](#).

²⁶ [GAO-14-713](#).

savings on as many as 67 data centers because of difficulties, such as calculating baseline data center costs. Further, we found that OMB had developed metrics, but these metrics do not address server utilization. Consequently, we recommended that OMB, among other things, develop and implement a metric for server utilization and agencies address their challenges in reporting costs savings. OMB and the agencies agreed with our recommendations. We have initiated follow-up efforts to assess agency progress in implementing our recommendations.

Agency CIOs Are to Address 36 IT Management Reporting Requirements for OMB

OMB directs agency CIOs to respond to 36 IT management reporting requirements.²⁷ These 36 requirements—which we organized by key IT management areas such as IT strategic planning, IT security, and related initiatives²⁸—are shown in table 1 along with

- a description of each requirement;
- how often (i.e., the frequency) required information is to be reported (e.g., monthly, quarterly, annually); and
- how agencies are to report required information (the reporting mechanism). OMB specifies for each requirement, the reporting mechanism to be used, which range from posting information on an agency's website or OMB's IT Dashboard to transmitting it to OMB via the MAX Portal or the Integrated Data Collection system.

Additional details about these requirements, including when each requirement and its associated OMB guidance was initiated, are provided in appendix II.

²⁷Since there could be several requirements for information in multiple OMB memorandums for one initiative, we grouped the requirements to report information together by initiative and the frequency of reporting rather than list each as its own separate requirement, which affected the total number of requirements identified.

²⁸These initiatives include various OMB-led federal IT efforts aimed at, among other things, making certain agency data publicly available, and e-government. We categorized these as related initiatives, because while they are important to IT management, they did not fit in the other key areas.

Table 1: CIO Reporting Requirements with Description, Reporting Frequency, and Mechanism, as of March 2014

Key area	Requirement and description	Frequency	Reporting mechanism
IT strategic planning	1. Information Resources Management strategic plan. Submit an updated Information Resources Management strategic plan that describes how the agency is applying information resources to improve the productivity, efficiency, and effectiveness of government programs.	As needed	Agency website
	2. Enterprise roadmap. Submit an updated Enterprise Roadmap that aligns with the Information Resources Management strategic plan and documents an agency's current and future views of its business and technology environment from an architecture perspective.	Annually	Agency website
Capital planning and investment management	3. Exhibit 53. Submit exhibit 53s for all major and non-major IT investments, which represent the agency's complete IT portfolio and include investment costs and performance benefits for each investment. These also include other IT investment-related information, such as the amount agencies are spending on cloud computing.	Annually, and multiple times as required ^a	IT Dashboard
	4. Exhibit 300. Submit an exhibit 300 for each major IT investments, which is a business case that provides investment information, including general information and planning for resources such as staffing and personnel, and provides more information, such as projects and activities.	Monthly, annually, and multiple times as required ^a	IT Dashboard
	5. Major IT investment documentation. Submit investment documents, artifacts, and associated metadata for all major IT investments, including a risk management plan, investment-level alternative analysis, and operational analyses.	Annually and as needed	Data Point ^b
	6. IT capital plan. Submit an IT capital plan, which is the agency's implementation plan for the budget year. ^c	Monthly, annually, and multiple times as required	IT Dashboard
	7. PortfolioStat progress report. Report on the progress of action items identified during past PortfolioStat sessions with OMB.	Quarterly	Meeting with OMB officials
	8. PortfolioStat review. Report on the agency's successes, challenges, and lessons learned throughout the PortfolioStat process.	One-time ^d	E-mail
	9. Compliance failures: Report to OMB instances of alleged failure to comply with the requirements in OMB's policy on the management of federal information resources (i.e., Circular A-130), which includes capital planning and investment control, and the resolution of these failures.	Annually	Meeting with OMB officials
IT security	10. IT security key metrics. Report on compliance with requirements to report certain security breaches to the United States Computer Emergency Readiness Team within 1 hour, as well as on progress in meeting OMB's 2012 and 2014 Internet protocol version 6 milestones.	Quarterly	Integrated Data Collection

Key area	Requirement and description	Frequency	Reporting mechanism
Systems acquisition, development, and integration	11. Cybersecurity performance improvements. Report on efforts to improve cybersecurity performance by focusing on what data and information are entering and exiting networks, what components are on information networks and when security status changes, and who is on the systems. ^e	Monthly and quarterly	CyberScope
	12. Federal Risk and Authorization Management Program key metrics. Submit a listing of all cloud services that an agency determines cannot meet the Federal Risk and Authorization Management Program security authorization requirements, with appropriate rationale and proposed resolutions.	Quarterly and annually	Integrated Data Collection
	13. Government-wide tracking of resources for cyber activities. Submit resource data on federal cybersecurity activities for fiscal years 2012 through 2015 and updated information in subsequent fiscal years, including federal and contractor full-time equivalent data.	Quarterly and annually	MAX Portal
	14. Information security continuous monitoring dashboard. Submit security-related information continuously via automated data feeds in accordance with requirements provided by the Department of Homeland Security, in coordination with OMB.	Continuous	Information Security Continuous Monitoring Dashboard ^f
	15. Monthly IT security data feeds. Submit data from automated security management tools.	Monthly	CyberScope
	16. IT security quarterly reporting. Submit responses to IT security posture questions, which address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.	Quarterly (1st, 2nd and 3rd only)	CyberScope
	17. Annual Federal Information Security Management Act report. Provide a report on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the act. ^g	Annually	CyberScope
	18. Cybersecurity plan of action. Submit quarterly and fiscal year targets for improving specific cybersecurity capabilities, based on recommendations from the Department of Homeland Security, and demonstrate progress toward those targets as programs mature.	Quarterly and annually	E-mail
	19. Personal Identity Verification credentials report (HSPD^h 12): Provide a report on the number of personal identity verification credentials issued to, among others, employees, and contractors.	Quarterly	Agency website
	20. Trusted Internet Connections initiative. Provide updates to the Department of Homeland Security on the agency's trust internet connections plans of action and milestones until they are completed.	Semi-annually	CyberScope
	21. Report significant IT security deficiencies: Report significant deficiencies identified under the Federal Information Security Management Act.	Annually	MAX Portal and Agency website
22. IT investment baseline updates. Notify OMB of cost and schedule baseline updates for major IT investments.		As needed	IT Dashboard

Key area	Requirement and description	Frequency	Reporting mechanism
	23. IT investment performance updates. Provide updated cost and schedule data for major investments on a monthly basis; performance measurement data when actual data have been measured (annually, at a minimum); and CIO assessments and contract data when significant changes occur.	Monthly, annually, and as needed	IT Dashboard
	24. Agency TechStat outcomes. Report the results of TechStat sessions—an agency-led process to terminate or turn around IT investments that are failing or are not producing results.	Quarterly	Integrated Data Collection
	25. Cloud First. Report on the implementation of the Cloud First policy, including the adoption of infrastructure-as-a-service, platform-as-a-service, and software-as-a-service solutions. ⁱ	Monthly, annually, and multiple times as required	IT Dashboard
	26. Commodity IT baseline update. Report on the efficiency of IT acquisitions efforts, including the number and types of planned commodity acquisitions, the extent to which an agency leverages enterprise-wide license agreements, and any duplication which may exist across agency IT acquisition efforts.	Quarterly	Integrated Data Collection
	27. Mobile contracts inventory update. Report on mobile and wireless service contract inventory by providing current prices for differentiated levels of voice, text, and data services contrasted to the number of devices for each major mobile operating system.	Quarterly	Integrated Data Collection
Related initiatives			
	28. Cost savings/avoidances. Report actual and planned cost savings and/or avoidances achieved or expected through the implementation of IT investments and related IT reform initiatives (e.g., data center consolidation, migration to shared services and cloud solutions) supported by Information Resources Management strategic plans and Enterprise Roadmaps.	Quarterly	Integrated Data Collection
	29. Data center closures/status update. Provide information on the agency's data centers, including the number of core and non-core data centers, agency progress on closures, and the extent to which agency data centers are optimized for total cost of ownership.	Annually	Federal Data Center Consolidation Initiative program management office portal ^j
	30. E-Government status report. Report on status of its implementation of e-government initiatives, compliance with the E-Government Act, and how e-government initiatives of the agency improve performance in delivering programs to constituencies.	Annually	MAX Portal
	31. Open Government directive. Publish an Open Government plan that describes how the agency will improve transparency and integrate public participation and collaboration into its activities.	Biennial	Agency website
	32. Open data policy enterprise inventory. Submit an enterprise-wide data inventory, and an inventory schedule that describes, among other things, how the agency will ensure that all data assets have been identified and accounted for in the inventory and how the agency plans to expand, enrich, and open its inventory.	Quarterly, as needed	Agency website
	33. Open data policy public data listing. Publish a list of agency data assets that are or could be made available to the public.	Quarterly	Agency website

Key area	Requirement and description	Frequency	Reporting mechanism
	34. Open data policy customer feedback process. Create and report a process for the agency to engage with customers through the agency.gov/data pages and other appropriate channels.	Quarterly	Agency website
	35. Open data policy data publication process. Publish an overview of the agency's data publication process, including the actual process by which data are determined to have a valid restriction to release and examples of what kinds of characteristics a data asset has that leads to a determination to not release.	Quarterly	Agency website
	36. Agency points of contact. Provide agency points of contact for various responsibilities, such as for PortfolioStat and Capital Planning.	Quarterly	Integrated Data Collection

Source: GAO analysis. | GAO-15-106

^aEach year OMB establishes a schedule for agencies to provide various iterations of these documents as it develops the federal budget.

^bData Point is an OMB web portal, similar to MAX Portal, that is used by agencies to submit documents.

^cThe IT capital plan is submitted by agencies as a part of their exhibit 53 submissions.

^dOMB required agencies to submit this report 2 weeks after the transmittal of the fiscal year 2015 budget to Congress (the budget was submitted on March 4, 2014). We included this one-time reporting requirement because it existed as of March 2014, which was within our period of work.

^eThe improve cybersecurity performance information is provided by agencies as a part of other IT security requirements submitted via CyberScope, such as the IT security metrics requirement.

^fThe Information Security Continuous Monitoring Dashboard is to be established by the Department of Homeland Security to provide agencies with a mechanism to report IT security-related information, including the management of software, hardware, configuration settings, and common vulnerabilities. The purpose of the dashboard is to help the department manage the highest priority and most serious risks to federal agencies.

^gAlthough OMB has incorporated agency reporting on privacy-related issues into annual Federal Information Security Management Act reporting, we have not included privacy since it was considered outside the scope of our work. See app. I for more details.

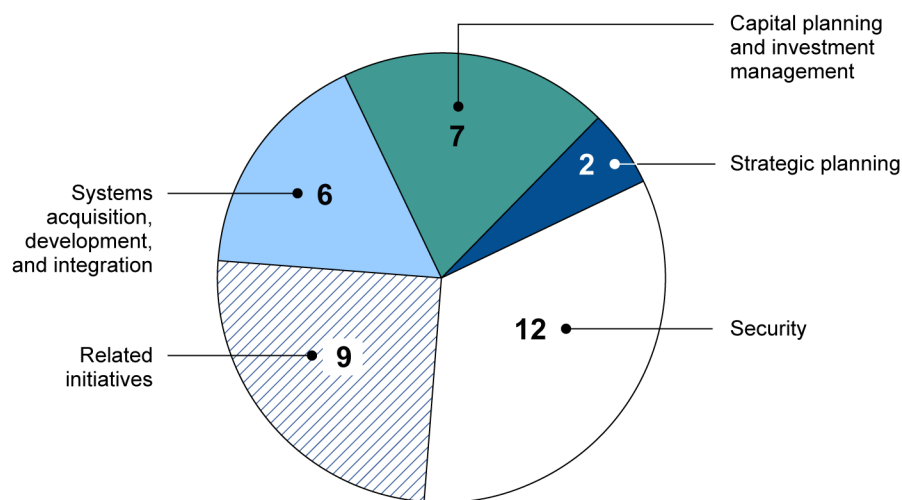
^hHSPD—Homeland Security Presidential Directive.

ⁱThe Cloud First information is submitted by agencies as part of their exhibit 53s.

^jThe Federal Data Center Consolidation Initiative program management office portal is a web portal established by the General Services Administration to be used by agencies to submit information related to data center consolidation efforts.

As shown in figure 1, of the 36 requirements, the largest number are in IT security (12), and the fewest are in IT strategic planning (2).

Figure 1: Number of Requirements per Key IT Management Area



Source: GAO analysis. | GAO-15-106

In terms of reporting frequency, agency CIOs are largely required by OMB to report on the 36 requirements on a quarterly or annual basis. Specifically, 29 of the 36 requirements are required to be reported quarterly and/or annually. Further, several requirements are required to be reported at multiple periods. For example, the cybersecurity plan of action is required to be reported both quarterly and annually. In addition, agencies are required to submit major IT investment documentation annually and as needed (e.g., when significant changes occur to an investment).

The other seven are to be reported as follows:

- one biennially,
- one semi-annually,
- one monthly,
- one one-time,
- one continuously, and
- two as-needed.

According to officials from OMB's Office of E-Government and Information Technology, OMB established the particular reporting periods to ensure it gets the information that it needs at the proper time to achieve its mission to, among other things, develop the President's budget, make

informed policy decisions, provide oversight, and meet statutory requirements. For example, OMB requires agencies to report quarterly on cost savings and avoidances, which assists OMB in publishing its quarterly report to Congress on progress with IT oversight and reform.²⁹ Further, OMB requests that agencies report annually on the implementation status of their e-government initiatives, which assists OMB in developing its annual report to Congress on federal e-government.³⁰ OMB also requests certain requirements to be reported at multiple periods. For example, agencies are required to report multiple iterations of their exhibits 53s and 300s in accordance with a schedule developed by OMB, which assists OMB in developing the President's budget.

OMB has the agencies report these requirements via four primary mechanisms—namely, the federal IT Dashboard, the Department of Homeland Security's CyberScope portal, OMB's Integrated Data Collection system, and agency websites. More specifically, of the 36 requirements, agencies use

- the federal IT dashboard for 6 requirements,
- CyberScope for 5 requirements,
- the Integrated Data Collection system for 7 requirements, and
- agency websites for 9 requirements.

Agencies also report eight requirements using other mechanisms, including

- one via Data Point,
- one via a Department of Homeland Security information security continuous monitoring dashboard,
- one via the Federal Data Center Consolidation Initiative program management office portal,
- two via meetings with OMB officials,
- three via MAX Portal, and

²⁹OMB, *Quarterly Report to Congress: Information Technology Oversight and Reform* (Washington, D.C.: May 6, 2014).

³⁰OMB, *Fiscal Year 2013 Annual E-Government Act Initiatives* (Washington, D.C.: March 1, 2014).

-
- two via e-mail.³¹

In terms of OMB's IT reform initiatives, there are a number of the 36 requirements related to managing and overseeing OMB's efforts in these areas. Key examples include the requirements on:

- Agency TechStat outcomes,
- Data center closures/status update,
- PortfolioStat progress report,
- PortfolioStat progress review, and
- Commodity IT baseline updates.

Although OMB Uses Required Information, CIOs Reported That the Majority of Reporting Requirements Are Not Useful for Managing IT and Identified Areas for Improvement

OMB uses the information reported by CIOs with the goal of improving the management, oversight, and transparency of the federal government's IT, but CIOs reported that addressing the majority of the reporting requirements was not useful for managing IT.³² Specifically, the majority of the 24 agency CIOs surveyed that responded reported that 4 of the 36 reporting requirements helped to a very great or great extent in managing IT and 8 requirements helped to a moderate extent. The remaining 24 reporting requirements only help agency CIOs some to no extent. The CIOs also reported that meeting the reporting requirements took a significant level of effort to implement, including spending totaling approximately \$150 million to \$308 million each year. According to comments from a number of CIOs, they did not always find these requirements helpful because addressing them did not always clearly support departmental priorities and they were burdensome due in part to the reporting format, frequency, and duplicative nature of certain elements. Additionally, to improve the effectiveness of requirement reporting, at least 8 CIOs proposed changing 13 reporting requirements (e.g., changing the frequency of reporting or eliminating requirements) and improving OMB's feedback to agencies on requirements.

Nonetheless, our recent reports³³ provide evidence that requirements associated with OMB's IT reforms—specifically, TechStat, data center

³¹One requirement, report significant IT security deficiencies, is reported via both MAX Portal and agency websites.

³²For the purposes of this report, when we refer to CIO responses, they include those responses provided directly by CIOs and those provided by agency officials on behalf of CIOs.

³³See, for example, [GAO-13-524](#), [GAO-14-713](#), and [GAO-14-65](#).

consolidation, and PortfolioStat—still have important value. Accordingly, it is concerning that CIOs do not always see value in these reporting requirements. Consequently, effectively addressing proposed changes and aligning CIOs' priorities to OMB's (i.e., establishing a common understanding of what the priorities are) is important to, among other things, the success of OMB's reforms and its goal of improving federal IT. Until this is done, there is a risk that the IT reforms will not succeed.

OMB Utilizes Reported Information to Meet Its Responsibilities

According to officials from OMB's Office of E-Government and Information Technology, OMB utilizes all the information reported by agency CIOs to carry out, among other things, its budget development, policy formulation, and oversight roles and responsibilities. Specifically, it uses the information to undertake the following activities:

- **Development and execution of the President's budget.**³⁴ Each year, OMB and federal agencies work together to determine how much the government plans to spend on IT projects and how these funds are to be allocated. OMB coordinates with federal agencies to obtain agency budget requests, and other information through the exhibit 53, exhibit 300, and annual FISMA reporting. OMB uses this information to analyze the requests, and prepare budget materials for the President's review. These budget materials also include an analytical assessment that, among other things, provides details on the federal IT budget and the administration's key federal IT initiatives.³⁵
- **Formulation of policies and guidance for the management of federal agency IT.** OMB issues policy guidance and memorandums related to various aspects of IT management in order to improve the management, oversight, and transparency of the federal government's IT. As part of these activities, OMB uses the information reported by agencies to inform policy decisions. For instance, OMB uses the reported information from the Federal Risk and Authorization

³⁴The President's budget is the Administration's proposed plan for, among other things, setting levels of spending, managing funds, and financing the spending of the federal government. It is not only the President's principal policy statement but is also the starting point for congressional budgetary actions.

³⁵For the fiscal year 2015 assessment, see OMB, *Analytical Perspectives, Budget of the U.S. Government, Fiscal Year 2015* (Washington, D.C.: 2014).

Management Program to evaluate agency progress in implementing cloud services, which is an OMB policy priority.

- **Oversight of federal agency IT.** OMB's Office of E-Government and Information Technology is also responsible for oversight of federal information technology spending, and more than \$80 billion is annually invested in federal IT. OMB provides oversight through several mechanisms including the Federal IT Dashboard, PortfolioStat reviews, and TechStat sessions. For instance, OMB requires agencies to report information on their IT portfolio, including commodity IT baselines, and information related to the Federal Information Security Management Act, as well as develop an Information Resources Management Strategic Plan and Enterprise Roadmap. OMB's goal is to use the information it collects from agencies to monitor federal IT spending and help ensure programs and operations are efficient and effective.
- **Meeting statutory requirements.** Under federal law, OMB's Office of E-Government and Information Technology is required to report to Congress on certain IT management areas. In particular, the office is required to submit a report on the implementation of the E-Government Act of 2002,³⁶ which summarizes information reported by agencies as required under the act. In addition, during the period of our review, OMB was also required to submit a report on the implementation of the Federal Information Security Management Act of 2002³⁷ by federal agencies. In order to prepare these reports, OMB requires agencies to submit information on their implementation efforts as required under the acts, which OMB then summarizes for Congress.

³⁶44 U.S.C. § 3606. See OMB, *FY13 Report to Congress on the Implementation of the E-Government Act of 2002* (Washington, D.C.: Mar. 1, 2014).

³⁷The OMB report was required by the Federal Information Security Management Act of 2002, at 44 U.S.C. § 3543(a)(8). As previously noted, in December 2014, as our review was finishing, the 2002 act was largely superseded by the Federal Information Security Modernization Act, which contains a similar OMB reporting requirement at 44 U.S.C. § 3553(c).

CIOs Identified Reporting Requirements Most Useful for Managing IT and Those That Were Less Useful

The 24 agency CIOs we surveyed reported that addressing certain reporting requirements assisted their agency in managing IT, while addressing other reporting requirements were not as useful. Specifically, a majority of 24 CIOs surveyed that responded reported that addressing 4 reporting requirements helped their agency to manage IT to a very great extent or great extent and 8 helped the agency to manage their IT to a moderate extent. They also reported that addressing the 24 remaining reporting requirements helped agencies only to some to no extent in managing IT.

Table 2 lists the 36 reporting requirements by the extent of assistance in managing IT as reported by agency CIOs. Specifically, it shows how the majority of CIOs (including the number) rated each requirement against our categories of usefulness—either very great to great, moderate, or some to no extent.

Table 2: Extent to Which Addressing the 36 Reporting Requirements Is Useful to Managing IT

Usefulness	Requirement	Number Reporting
Very great to great extent	Information Resources Management strategic plan	14
	Enterprise roadmap	12
	Exhibit 53	12
	IT investment performance updates	10
Moderate extent	Exhibit 300	8 ^a
	Report significant IT security deficiencies	5 ^b
	IT security key metrics	10
	Monthly IT security data feeds	9
	IT security quarterly reporting	10
	Annual Federal Information Security Management Act report	10
	Information security continuous monitoring dashboard	7 ^c
	IT investment baseline updates	8 ^d
Some to no extent	Major IT investment documentation	10
	IT capital plan	13
	Compliance failures	14
	PortfolioStat progress report	13
	PortfolioStat review	13
	Cybersecurity performance improvements	11

Usefulness	Requirement	Number Reporting
	Federal Risk and Authorization Management Program key metrics	13
	Government-wide tracking of resources for cyber activities	15
	Cybersecurity plan of action	10
	Cost savings/avoidances	11
	Agency TechStat outcomes	9
	E-Government status report	14
	Personal Identity Verification credentials report (Homeland Security Presidential Directive 12)	14
	Trusted Internet Connections initiative	9
	Open Government directive	13
	Commodity IT baseline updates	10
	Mobile contracts inventory update	11
	Data center closures/status update	9
	Cloud First	12
	Agency points of contact	19
	Open data policy enterprise inventory	11
	Open data policy public data listing	12
	Open data policy customer feedback process	18
	Open data policy data publication process	17

Source: GAO survey of 24 Chief Financial Officer Act agency chief information officers. | GAO-15-106

Note: The number of agency chief information officers that responded to our question on the extent to which a requirement assisted the agency in managing IT was less than 24 for 33 requirements.

^aFor the exhibit 300, there were eight respondents for each level of usefulness. Therefore, the moderate category was selected as the best representation of overall views.

^bFor reporting significant deficiencies, there were 21 respondents to this question (8 very great to great, 5 moderate, 8 some to no extent). The moderate category was selected as the best representation of overall views.

^cFor the security dashboard, there were 22 respondents to this question (8 very great to great, 7 moderate, and 8 some to no extent). The moderate category was selected as the best representation of overall views.

^dFor the investment baseline updates, there were 23 respondents to this question (8 very great to great, 8 moderate, and 7 some to no extent). The moderate category was selected as the best representation of overall views.

In addition, of the 24 requirements that CIOs found only assisted their agency in managing IT to some to no extent, our analysis showed that a number of them were associated with OMB's IT reform initiatives. In particular, they include the requirements on

- Agency TechStat outcomes,

-
- Data center closures/status update,
 - PortfolioStat progress report,
 - PortfolioStat progress review, and
 - Commodity IT baseline updates.
-

CIOs Reported That Addressing Requirements That Were Not Always Useful Took a Significant Level of Effort to Implement

With regard to effort required to meet the 36 reporting requirements, the majority of the 24 agency CIOs reported that

- 16 requirements required a very great or great effort to meet,
- 14 required a moderate effort, and
- 6 required some to no effort to meet.

In addition, in terms of resources, agency CIOs estimated that they spend in total, approximately \$150 million to \$308 million annually to address the 36 reporting requirements. For individual requirements, agencies' estimates of the range spent were generally at least a total of \$1 million annually and as high as \$19 million for one requirement (exhibit 300).

The majority of the 24 agency CIOs that responded also reported that the level of effort and resources reported to meet the requirement was sometimes greater than the extent to which addressing the reporting requirement assisted the agency in managing their IT. Specifically, of the 24 reporting requirements that provided some to no assistance in managing IT, 8 of these required very great or great effort to meet and 10 required moderate effort to meet. In addition, 4 of the 8 reporting requirements that helped agencies to a moderate extent in managing IT required a very great to great effort to meet.

Further, 26 out of 36 reporting requirements that CIOs reported assisted agencies in managing IT to some or no extent were estimated to cost agencies approximately \$76 million to \$164 million each year to meet. In addition, the 8 requirements that assisted agencies to a moderate extent were estimated to cost approximately \$50 million to \$92 million a year. However, the 4 key reporting requirements that helped agencies manage their IT to a very great or great extent were estimated to cost \$24 million to \$52 million a year.

Table 3 lists the 36 reporting requirements by the CIO reported usefulness of assistance in managing IT, the level of effort required, and the estimated annual cost to meet the requirement. More specifically, it shows how the majority of CIOs that responded rated each requirement against our categories of levels of effort—either very great to great, moderate, or some to no effort.

Table 3: Reporting Requirements by Chief Information Officer-Reported Usefulness in Assisting in Managing Agency IT, Level of Effort, and Estimated Total Annual Cost

Usefulness	Requirement	EFFORT			Total cost (mil)
		Very great to great	Moderate	Some to no effort	
Very great to great extent	Information Resources Management strategic plan	✓			\$3-9
	Enterprise roadmap	✓			\$4-12
	Exhibit 53	✓			\$9-18
	Information technology (IT) investment performance updates	✓			\$8-13
Moderate extent	Exhibit 300	✓			\$10-19
	Report significant IT security deficiencies	✓			\$4-8
	IT security key metrics		✓		\$4-8
	Monthly IT security data feeds		✓		\$6-11
	IT security quarterly reporting	✓			\$5-11
	Annual Federal Information Security Management Act report	✓			\$7-13
	Information security continuous monitoring dashboard		✓		\$8-11
	IT investment baseline updates		✓		\$6-11
	Major IT investment documentation	*			\$9-15
Some to no extent	IT capital plan		✓		\$3-8
	Compliance failures			✓	\$1-4
	PortfolioStat progress report		✓		\$4-8
	PortfolioStat review	*			\$3-7
	Cybersecurity performance improvements	*			\$8-12
	Federal Risk and Authorization Management Program key metrics		✓		\$2-5
	Government-wide tracking of resources for cyber activities	*			\$6-10
	Cybersecurity plan of action		✓		\$3-8
	Cost savings/avoidances	*			\$3-9
	Agency TechStat outcomes			✓	\$1-3
	E-Government status report		✓		\$2-5
	Personal Identity Verification credentials (HSPD 12)			✓	\$1-4
	Trusted Internet Connections initiative		✓		\$3-6
	Open Government directive	*			\$2-5
	Commodity IT baseline updates	*			\$6-10
	Mobile contracts inventory update		✓		\$2-5
	Data center closures/status update		✓		\$4-8
	Cloud First		✓		\$1-4
	Agency points of contact			✓	\$1-2
	Open data policy enterprise inventory	*			\$5-10
	Open data policy public data listing		✓		\$3-6
	Open data policy customer feedback process			✓	\$2-6
	Open data policy data publication process			✓	\$2-4
Totals		16	14	6	\$150-308

Source: GAO survey of 24 CFO Act Agency CIOs. | GAO-15-106



Some to no usefulness and very great to great effort

In addition to the fact that a majority of the 24 agency CIOs that responded reported that complying with many of the reporting requirements was not always commensurate with their usefulness in managing IT, they also generally indicated they would only collect at least some, but not all of the information, if addressing the requirements was optional. Specifically, for the 24 requirements that helped some to no extent, the majority of the CIOs reported that they would collect at least some but not all of the information if not required to do so.

According to comments from a number of CIOs, they did not always find that these requirements were useful because addressing them did not always clearly support departmental priorities. For example, with regard to reporting investment information using the exhibit 300, three CIOs said it had little value beyond reporting information that OMB needed to make decisions because their departments had their own processes for investment decisions. For IT security quarterly reporting and monthly IT security data feeds, three CIOs said these requirements were not commensurate with their usefulness because they were burdensome due in part, to the reporting format, frequency, and duplicative nature of certain elements. Other examples cited by CIOs include the following:

- For government-wide tracking of cybersecurity resources, one agency CIO commented that it was helpful to determine how much funding was spent on cybersecurity, but providing the supporting detailed accounting of the resources called for in the requirement was difficult. Another CIO commented that tracking resources helped in understanding the investments made and historical data provided insight into whether prior allocated resources were impactful; however, the reporting requirement needed to be consolidated with annual Federal Information Security Management Act reporting.
- Concerning commodity IT baseline updates, one agency CIO commented that it had helped with understanding the types of commodity spending that made up the agency's portfolio and identified opportunities for optimization but reporting needed to be combined with other annual budget reporting. Another CIO commented that while reporting this information helped OMB provide oversight, the agency would prefer if OMB used the information to help agencies develop better strategies and operations plans that would result in cost reductions.
- Regarding program management cost savings and avoidances, an agency CIO commented that while tracking cost savings provides a

more robust understanding of its IT portfolio, the reporting is too frequent for capturing the cost savings. Another CIO noted that the reporting helps identify initiatives that are successful in driving down costs and those that are falling short of projected savings, but providing updates on changes to the cost savings and avoidance figures to OMB is burdensome.

CIOs Proposed Changes to Improve Reporting Requirements and OMB Feedback

Although agency CIOs surveyed generally found some of OMB's initiatives valuable for managing IT resources, at least 8 or more proposed changes to improve (1) 13 reporting requirements and (2) OMB's feedback to agencies on the reporting requirements generally.

With regard to the 13 reporting requirements, at least nine agency CIOs proposed changing what information should be reported under 3 reporting requirements, stating that data elements that do not add value in terms of what OMB needs or uses to make decisions or are no longer relevant should be removed. Agency CIOs also proposed changing the frequency of reporting for 5 requirements, moving from reporting on a quarterly basis to either a semi-annual or annual basis. In addition, at least eight of the CIOs proposed that 4 reporting requirements should be eliminated because they were generally either not useful to the agencies in managing their IT, information was duplicative with other reporting requirements, or OMB had not requested the information in recent years. Table 4 lists the reporting requirements, the agency CIOs' proposed changes, and the number of CIOs that proposed them.

Table 4: Agency Chief Information Officer (CIO) Proposed Changes to Reporting Requirements

Reporting Requirement	Type of change	Proposed change and rationale	Number of CIOs reporting
1. Exhibit 300	Change what information is reported	<p>Remove data elements that do not add value (i.e., only what OMB really needs or uses to make decisions) or do not provide value in monitoring/oversight of investments.</p> <p>Limit changes to what is included in exhibit 300 to allow for comparisons and trending over years.</p> <p>Remove data that are already reported elsewhere (e.g., contract/acquisition information, which is reported through the Federal Procurement Data System).</p> <p>Allow for reporting on investment components.</p>	13

Reporting Requirement	Type of change	Proposed change and rationale	Number of CIOs reporting
2. Exhibit 53	Change what information is reported	Remove data elements that do not add value (i.e., only what OMB really needs or uses to make decisions) or are no longer relevant. Agencies should be given the option to only provide an update if a change occurs. Should reflect only agency-received funding and support the request for funding (should not be used as a catch-all for other data collection).	10
3. Annual Federal Information Security Management Act report	Change what information is reported	Remove data elements that do not add value (i.e., only what OMB and the Department of Homeland Security really need or use to make decisions), do not provide value in monitoring/oversight of security (i.e., those that do not provide useful performance metrics), or are not related to what is required under the law. Remove questions that duplicate information collected through other mechanisms on a more frequent basis. Reporting guidance needs to be published earlier.	9
4. Cost savings/avoidances	New frequency of reporting	Change from quarterly to annually. Move to annual reporting to help limit the number of changes that OMB makes to what information should be reported throughout the year. Calculating savings and avoidances for these types of activities is not appropriate on a quarterly basis due to the time involved in transitioning resources.	11
5. Commodity IT baseline updates	New frequency of reporting	Change from quarterly to semi-annually. Move to semi-annual reporting to help reduce (1) the burden of reporting data that change very little from one quarter to the next, and (2) the effort required to manually enter the data into the MAX Portal. Should align or be consolidated with the annual exhibit 53 process.	10
6. PortfolioStat progress report	New frequency of reporting	Change from quarterly to either semi-annually or annually. Should be a frequency that is agreed upon between OMB and the agency.	9
7. Cloud First	New frequency of reporting	Change from quarterly to either semi-annually or annually. Should align with reporting of other initiatives with related goals and the exhibit 53 process.	9
8. Open data policy publication process	New frequency of reporting	Change from quarterly to annually. Should align with reporting of other initiatives with related goals.	9
9. Open Government directive	Consolidate or combine with other requirements	Consolidate with other Open Data policy reporting and/or Digital Government Strategy. Consolidate to be included in Agency Strategic Plan and/or Enterprise Roadmap.	8
10. Major IT investment documentation	Eliminate requirement	Provides no value to the agency's management of IT, and it is not clear what value agencies would gain from OMB feedback. OMB has not clarified why it is collecting this information or how it will be utilized.	9
11. IT capital plan	Eliminate requirement	OMB has not requested this information for recent submissions. Information is reported elsewhere in other requirements.	9

Reporting Requirement	Type of change	Proposed change and rationale	Number of CIOs reporting
12. E-Government status report	Eliminate requirement	Provides no value to the agency's management of IT. Some data elements are reported elsewhere in other requirements or through other mechanisms.	9
13. Compliance failures	Eliminate requirement	Agencies have not provided this information in recent years, and OMB has not requested this information. Information is reported elsewhere in other requirements.	8

Source: GAO survey of 24 CFO Act Agency CIOs. | GAO-15-106

Officials from OMB's Office of E-Government and Information Technology stated that they had received similar feedback on proposed changes to the reporting requirements in the past. They said that in some cases there was confusion among agency officials regarding the reporting requirements. Officials noted that the feedback on the requirements was useful information but provided no specific plan or date for addressing these suggestions. Effectively addressing such proposed changes is important to improving the efficiency and effectiveness of reporting requirements and could better position OMB to achieve its goal of improving management, oversight, and transparency of federal IT. Until this is done, OMB risks requiring agencies to implement and report on requirements that are duplicative, wasteful, or inefficient.

With regard to improving feedback on reported information, agency CIOs suggested that OMB's feedback process could be improved. In particular, while agency CIOs reported that OMB provided feedback to them on the majority of the 36 reporting requirements, the majority of CIOs reported that the feedback was moderately effective to not effective for most reporting requirements. Six agency CIOs also reported that they were specifically interested in receiving better feedback on two reporting requirements—namely, the major IT investment documentation and the Open Government directive. The Office of E-Government and Information Technology officials stated that the information on the feedback, particularly those requirements agency CIOs were interested in receiving feedback on, was useful; nevertheless, the officials acknowledged that they do consistently not provide this level of feedback to the CIOs because in part, they did not know until now that the CIOs wanted feedback to this extent. Having a process that consistently provides effective feedback is key to helping agency CIOs better manage their IT resources and improve reporting; it is also consistent with OMB's goals to improve federal IT management, oversight, and transparency. Until an effective feedback process is in place, there is a risk that agencies are managing their IT in a suboptimal manner.

As mentioned previously, our extensive experience at federal agencies and recent reports have shown that a critical component to ensuring OMB's effective management and oversight of key IT reform initiatives—specifically, TechStat,³⁸ data center consolidation,³⁹ and PortfolioStat⁴⁰—is agency reporting of current and accurate information about the status of these initiatives, including the extent of any financial savings. However, agency CIOs surveyed reported that requirements related to these IT reform efforts, including agency TechStat outcomes, data center closures/status updates, commodity IT baseline updates, and PortfolioStat reviews and progress reports, helped their agency to only some or to no extent in managing IT. It is concerning that CIOs do not always see the value in reporting information that is essential to reform initiatives aimed at improving IT management effectiveness, saving money, and avoiding unnecessary costs, especially since key aspects of a number of the reforms have also been recently incorporated into law.

Consequently, establishing a common understanding between OMB and the CIOs on the priority of the reporting and related initiatives is key to the success of OMB reforms. As part of this understanding, it is also important to address underlying reasons cited by CIOs regarding the usefulness of requirements, including when department priorities are reportedly different than OMB's and the burdensome and duplicative nature of requirements. Until such an understanding is established, there is a risk these important IT reforms, which are key to improving the efficiency and effectiveness of federal agency programs and operations, will not fully succeed.

³⁸[GAO-13-524](#).

³⁹[GAO-14-713](#).

⁴⁰[GAO-14-65](#).

OMB Has Initiated Efforts to Streamline Reporting, but They Do Not Address Challenges Reported by CIOs

OMB has taken steps to streamline CIO reporting requirements. Specifically, OMB has initiated efforts to identify opportunities to change the format for reporting (e.g., from narrative-intensive descriptions to specific performance data) with the goal of reducing CIOs' reporting burden. Although these OMB efforts aim to streamline reporting, agency CIOs identified additional challenges with tracking what reporting requirements are currently in place, using multiple online tools to report required information, and using capital planning and investment reporting requirement information to make effective investment decisions, which are not addressed by OMB's efforts. This is in part to the fact that OMB has not solicited feedback in these areas because its priority has been on streamlining reporting in other areas (e.g., changing report formatting and others discussed below). By not addressing these CIO-identified challenges, OMB is missing opportunities to help CIOs improve the requirements reporting process and to improve its use of information collected as part of this process to effectively manage IT.

OMB Is Working to Streamline Reporting

OMB has initiated several efforts to streamline reporting:

- **Changing the format and mechanism of information that is submitted.** Officials from OMB's Office of E-Government and Information Technology reported that they are examining transitioning the reporting of certain requirements from previous narrative-intensive plans or other documentation into structured forms (such as the Integrated Data Collection) that call for specific data associated with OMB-established performance metrics. These officials stated that they are continually re-evaluating the format in which agencies should provide information in order to improve the efficiency of OMB's review process and the reliability of pertinent federal IT management data. For example, OMB expanded and refined its collection of key performance indicators for investment portfolio management with the Integrated Data Collection between 2013 and 2014.
- **Revising what information is currently required to be submitted as part of existing requirements.** The Office of E-Government and Information Technology officials stated that they recently began reviewing existing reporting requirements in the Integrated Data Collection prior to issuing quarterly reporting instructions to identify whether any elements should be changed. For example, in May 2014, as the result of one of these reviews, OMB removed the commodity IT baseline portion of the Integrated Data Collection for the submission due in November 2014. In addition, OMB reported it is working with

the CIOs to improve the value of agency reporting on the federal center consolidation initiative. Specifically, OMB reported that working via a task force that is part of the OMB-led CIO Council, OMB has helped to develop metrics and data collection requirements that best support administration goals associated with consolidating and optimizing data centers. OMB further reported that as a result of these efforts, it has made significant changes to both its reporting requirements and strategic approach associated with this initiative.

- **Incorporating lessons learned into the annual revision of PortfolioStat guidance.** The officials from the Office of E-Government and Information Technology also stated that in 2013 they initiated an annual review of lessons learned from agency PortfolioStat sessions to identify whether additional information is needed to improve the office's oversight of federal IT portfolio management. These officials added that they incorporated the results of these reviews into the 2014 PortfolioStat guidance, which may have included adding requirements or streamlining others. For example, OMB required agencies to identify IT investments that merit additional oversight and support for review and discussion during the 2014 PortfolioStat sessions. Selected agencies were required to develop an action plan with specific goals and targets for these high-impact investments.
- **Integrating requirements with other IT government-wide efforts.** The Office of E-Government and Information Technology officials added that they review existing requirements to identify potential changes, including opportunities to streamline, when new government-wide IT initiatives are introduced. For example, they reported that their office is currently in the process of evaluating CIO and other reporting requirements to determine how they align to OMB's strategic cross-agency priority goals associated with smarter

IT delivery, cybersecurity, and Open Data⁴¹ and whether there might be opportunities to further streamline existing reporting requirements.

In October 2013, OMB and the Federal CIO Council established a working group to streamline reporting requirements related to capital planning and investment control. The working group studied, among other things, whether IT investment performance information and related reporting to OMB could be streamlined and better aligned with what information was needed by CIOs to make informed investment decisions. As a result of the study, the working group made a number of short-term and long-term recommendations to OMB in April 2014 to improve its fiscal year 2016 IT budget capital planning guidance.⁴² According to OMB officials, they addressed certain short-term recommendations related to improving standard definitions and purchase provisions, and are working to address the long-term recommendations in future guidance. They also said they expect the working group to continue studying the issues associated with this area and to annually provide recommendations on improving and streamlining capital planning guidance.

OMB Efforts Do Not Address CIO-Identified Challenges in Meeting Reporting Requirements

Although OMB has initiated several efforts to further streamline CIO reporting requirements, its efforts do not address the following challenges agency CIOs identified in our survey in meeting reporting requirements:

Tracking what reporting requirements are currently in place can be confusing. Agency CIOs expressed confusion in our survey on whether certain reporting requirements (e.g., the IT Capital Plan and compliance failures) were still in effect. This confusion was due in part to neither OMB nor the majority of federal agencies we surveyed having a comprehensive list of current CIO and related reporting requirements. In particular,

⁴¹The GPRA Modernization Act of 2010 required OMB to establish cross-agency priority goals to address longstanding challenges where implementation required active collaboration between multiple agencies in order to improve progress. Three goals related to federal IT management were established: smarter IT delivery, cybersecurity and Open Data. The smarter IT delivery goal focuses on improving outcomes and customer satisfaction with federal services through smarter IT delivery and stronger agency accountability. The cybersecurity goal focuses on improving cybersecurity performance through ongoing awareness of information security, vulnerability, and threats. Open Data focuses on unlocking the value of government data and adopting management approaches that promote interoperability and openness of this data to fuel innovation and improve government efficiency.

⁴²OMB, *FY 2016 IT Budget-Capital Planning Guidance* (Washington D.C.: May 23, 2014).

officials from the Office of E-Government and Information Technology office noted that while they did not maintain a comprehensive list, they did have a spreadsheet they used for selected review processes (e.g., PortfolioStat) but that this list was not available to the federal agencies because it was an internal OMB working document. Having a comprehensive list of current CIO reporting requirements is important for agencies to effectively manage their resources and respond to these requirements and for OMB to effectively manage its streamlining efforts consistent with its goal of reducing CIO reporting burden. Without such a list, OMB may lack sufficient information to make informed decisions about streamlining efforts and agencies risk wasting resources responding to reporting requirements that have changed or are no longer in effect.

Having multiple online reporting tools takes additional time and resources to enter required information and can be duplicative.

Agency CIOs reported in our survey that having to enter data into multiple online tools for reporting required information as part of capital planning, system integration, and IT security takes additional time and resources and can be duplicative. OMB requires agencies to use three online tools (Data Point, IT Dashboard, and the Integrated Data Collection) as well as e-mail for capital planning and system integration reporting requirements, and four online tools (Cyberscope, MAX Portal, Integrated Data Collection, and the Information Security Continuous Monitoring Dashboard) for IT security. In particular, agency officials noted that certain information for the capital planning reporting requirements (exhibit 53, exhibit 300) and cybersecurity reporting requirements (IT security key metrics, monthly IT security data feeds, IT security quarterly reporting) must be entered, in accordance with OMB's direction, in each tool; some information must be reported by bureau or office; and there are limitations in uploading data using a spreadsheet or multiple attachments into the tools, all of which takes additional time and resources.

OMB officials stated that they were looking at what reporting requirements can be reported on through the tools, particularly the Integrated Data Collection, and what steps can be taken to simplify the tools. They also noted that there were challenges when determining whether to reuse an existing tool or create a new one for reporting requirements, particularly when they needed agencies to report information within a short time frame, but provided no specific date or plan for the completing the above described efforts, including addressing the related challenges. Having centralized tools for reporting required data is critical to reducing the reporting of duplicative data, as well as

reducing the time and resources required to enter the data, and would be consistent with OMB's goal of reducing CIO reporting burden. By not including efforts to streamline reporting tools as part of OMB's overall requirements streamlining effort, there is a risk that agencies will continue to expend valuable time and resources entering potentially duplicative data into multiple reporting tools.

Using capital planning and investment reporting requirement information does not provide information to make effective investment decisions. As mentioned previously, agency CIOs reported in our survey that six of the seven capital planning and investment reporting requirements—namely the exhibit 53, exhibit 300, major IT investment documentation, IT Capital Plan, PortfolioStat progress report, and compliance failures—needed improvement. For example, agency CIOs reported that the two key capital planning reporting requirements—the exhibit 53 and exhibit 300—needed to be improved to remove data elements that did not provide value in making decisions. For the exhibit 53, this included eliminating non-financial data elements, such as those on cloud computing, and for the exhibit 300, eliminating the contracts and acquisition information since it was reported elsewhere. In addition, agency CIOs proposed eliminating three of the capital planning and investment reporting requirements (e.g., major IT investment documentation, IT Capital Plan, and compliance failures) because agencies had either not provided this information in recent years or information was reported elsewhere in accordance with other reporting requirements. By not focusing on efforts to streamline and improve capital planning and investment reporting requirements, there is a risk that OMB will not be able to adequately respond to the evolving nature of IT and ensure these key reporting requirements include data elements that provide the necessary value in making critical investment decisions.

With regard to the above challenges, the OMB officials told us that they were not currently addressing them because their top concern was the other requirement streamlining areas (i.e., changing the format and incorporating lessons learned) they were focusing on. They added that they had not solicited feedback from the agencies in the areas that were the focus of our survey and thus were not aware of the challenges. The officials also noted that the feedback we provided from the CIO surveys, including the challenges currently faced by CIOs, was useful information to consider as part of their further streamlining efforts. Nonetheless, until these challenges are addressed, OMB risks not achieving its goal of reducing CIO reporting burden and is missing opportunities to help CIOs

improve the reporting process, and their use of information collected as part of this process, to effectively manage IT.

Conclusions

OMB has established an extensive framework of IT management reporting requirements to aid in carrying out its mission and to help federal agency CIOs manage their IT resources. Although OMB uses reported information to meet its responsibilities, the majority of the 24 CIOs for the most part, do not, citing that (1) two thirds of the reporting requirements are not very useful to them in managing IT and (2) addressing reporting requirements entails a significant effort on the part of the CIOs, including an annual multi-hundred-million-dollar financial commitment. Nonetheless, our extensive experience at federal agencies and recent work have shown that reporting requirements—in particular, those relating to TechStat, data center consolidation, and PortfolioStat—are key to carrying out OMB's IT reforms and their goal of improving federal agency programs and operations, including producing financial savings. Consequently, it is of particular concern that OMB and the CIOs are not fully aligned on the utility of reporting requirements integral to the success of OMB's reforms. This misalignment is due in part to a lack of a common understanding between OMB and the CIOs on the priority nature of these reporting requirements and their associated reforms. Without such a common understanding, OMB and the CIOs risk missing key opportunities to improve federal programs and operations and produce savings. The CIOs did propose a number of changes aimed at increasing the usefulness of reporting requirements and providing for effective feedback, but OMB had not yet established an effective approach to address them. Until it does, OMB risks requiring agencies to report on and manage IT in a suboptimal manner, which is inconsistent with its goal of improving federal IT management.

While OMB's efforts to streamline CIO reporting are steps in the right direction, they largely do not address the CIO-identified challenges discussed in this report. These challenges are not being addressed by OMB in part because it is focusing on other aspects of requirement streamlining as its top priority and also because of a lack of awareness of these specific CIO challenges. Until these challenges are addressed, OMB is missing opportunities to help CIOs improve the requirements reporting process and its use of information collected as part of this process to effectively manage IT.

Recommendations for Executive Action

To improve the effectiveness of OMB streamlining efforts and ensure agency CIOs are better able to carry out their responsibilities in managing IT, including implementing OMB's IT reform initiatives, we recommend the Director of OMB direct the Federal CIO, in collaboration with agency CIOs, to take the following four actions:

- Ensure there is a common understanding with agency CIOs on the priority of the current reporting requirements and related IT reform initiatives. This should include addressing underlying reasons cited by CIOs regarding the usefulness of requirements, including when department priorities are reportedly different than OMB's and the burdensome and duplicative nature of requirements.
- Address and incorporate, as appropriate, the 13 proposed improvements to reporting requirements made by agency CIOs in our survey. This should include developing milestones and associated plans for completing this effort.
- Ensure the feedback process on information reported by CIOs consistently provides effective and constructive responses to these officials on their reported information.
- Assess, as part of ongoing streamlining efforts, the reporting challenges identified in our report. This should include determining whether to (1) have a comprehensive list of current IT reporting requirements that is publically available to agency CIOs; (2) reduce the number of reporting tools; and (3) improve the utility of capital planning and investment reporting requirements, and taking steps to implement where appropriate.

Agency Comments and Our Evaluation

In written comments provided by the Federal CIO and reprinted in appendix IV, OMB stated it respectfully neither agreed nor disagreed with our recommendations. According to OMB, it chose to take no position on the recommendations due to its concerns that: (1) our draft report's count of reporting requirements was not currently accurate, (2) our survey approach did not fully support the report's findings and recommendations, (3) the second objective to solicit CIO views did not allow for sufficient context setting, and (4) OMB has taken steps to solicit feedback and streamline requirements that are not reflected in the draft report. OMB added that it agreed with the principles contained in the recommendations that stress the importance of a common understanding with CIOs and other key stakeholders on the importance and priority of reporting requirements, ensuring effective and constructive feedback to CIOs on

the reported information, and streamlining reporting requirements. OMB further noted that it has actively incorporated these principles in its work and continuously works to enhance its efforts in these areas.

We evaluated OMB's concerns and found them, as discussed below, in large part either unfounded or as having no material impact on our results and recommendations. Consequently, we stand by our findings on OMB's key IT reform initiatives—and their associated reporting requirements—which are critical to improving federal IT management effectiveness. Further, ensuring the success of these reforms is a key reason why Congress, in December 2014, incorporated key aspects of a number of these reforms into law.⁴³ Accordingly, we believe our recommendations to OMB are still valid and essential.

With regard to OMB's first concern about the accuracy of the number of requirements identified in our report, OMB took issue with our inclusion of seven requirements, although it provided no documentation to support its comments; specifically, OMB said

(1) two requirements did not exist at the time of GAO's audit (specifically, Information Security Continuous Monitoring Dashboard and Cybersecurity Plans of Action),

(2) two had been eliminated by OMB during or shortly after the audit time frame—namely, the PortfolioStat Review and the Commodity IT Baseline, and

(3) three appeared to have been double-counted (specifically, the IT Capital Plan and Cloud First are components of the Exhibit 53 requirement, and Open Data Policy Public Data Listing is a subset of Open Data Enterprise Inventory).

Regarding the first two requirements (Information Security Continuous Monitoring Dashboard and Cybersecurity Plan of Action), our analysis shows these requirements were in effect at the time of our audit, and this is why we therefore included them in our list. Specifically,

⁴³See, the federal information technology acquisition reform provisions (commonly referred to as the Federal Information Technology Acquisition Reform Act or FITARA) of the 2015 Defense Authorization Act.

-
- OMB memorandum M-14-03 (dated November 2013)⁴⁴ requires agencies, in addition to submitting data to this dashboard once it is deployed, to report on the status of their preparation for meeting this requirement starting in 2014, which was in the time frame specified in our scope and methodology.
 - OMB memorandum M-12-20 (dated September 2012) stated that The Department of Homeland Security will “ask agencies to complete a Plan of Action for improving specific cybersecurity responsibilities. Agencies will provide quarterly and fiscal year targets and demonstrate progress toward these targets as they mature their programs.” Although OMB assigned responsibility to the Department of Homeland Security for these plans and subsequent quarterly updates, we considered it to be an OMB reporting requirement because the reporting requirement was included in an OMB memorandum.

In addition, for the two requirements that OMB said were eliminated (i.e., PortfolioStat review and Commodity IT Baseline), our evaluation shows that both had not been eliminated as of March 2014, which is the “as-of” date specified in our scope and methodology. Specifically,

- OMB memorandum M-13-09 (dated March 2013) required agencies to submit a consolidated document of successes, challenges, and lessons learned to OMB no later than 2 weeks after the transmittal of the President’s Budget for fiscal year 2015 to Congress (which was sent on March 4, 2014). Since the requirement was in effect as of March 2014, we included it in our list.
- OMB memorandum M-13-09 also required agencies to provide a quarterly update of their commodity IT baseline to OMB. Because this requirement was not eliminated until May 2014, as OMB’s comments and our report indicated, we therefore included it in our list since the requirement was in effect as of March 2014.

Thirdly, although OMB stated that we double counted three requirements (i.e., IT capital plan, Cloud First, and the Open Data Policy Public Data Listing), the evidence shows otherwise. Specifically, these requirements

⁴⁴OMB, *Enhancing the Security of Federal Information and Information Systems*, M-14-03 (Washington, D.C.: Nov. 18, 2013).

are defined in OMB circulars or memoranda (as noted in appendix II) as separate reporting initiatives, and we therefore treated them as such. For example, the requirement for an IT capital plan is outlined in OMB Circular A-130 (dated November 2000)⁴⁵ and details several activities that the agency must provide annually to OMB as part of the budget submission.

In addition to the above, it is important to note that (as described in our report's scope and methodology) after we developed our list of requirements, we asked all 24 CFO agencies as well as OMB to review the list and provide feedback as a means to validate that our inventory was accurate. Specifically, we had officials from the 24 agencies review our list to ensure it was complete and accurate, adjusted our list as appropriate based on their feedback, and reached consensus on the number of requirements in the inventory. In the case of OMB, we had officials from the Office of E-Government and Information Technology review our list multiple times and adjusted our list as appropriate based on their feedback. During these OMB meetings, the officials never raised the specific issues OMB noted in its written comments.

It is also important to note that we took these validation steps because, as we noted in our report, OMB does not maintain a comprehensive list of current CIO reporting requirements. This has left agencies confused regarding what requirements were currently in place, and is therefore why we recommended that OMB develop such a list. This inconsistency among OMB's written response, what the agencies told us, and what OMB representatives previously told us confirms the need for GAO's recommendation.

OMB's second concern was that our survey approach did not fully support the report's findings and conclusions. Specifically, OMB stated that many agency CIOs told OMB through the CIO Council that they delegated full responsibility for completing the survey to lower-level staff and because of this, OMB did not have full confidence in some of our findings and felt our attributions was not appropriate. In addition to this concern, OMB said that it believed GAO gave disproportionate weight to the estimated costs reported, which appeared, in its opinion, to be unsubstantiated because they were based on a survey question that did not require the basic

⁴⁵OMB, *Management of Federal Information Resources*, Circular No. A-130 (Washington, D.C.: Nov. 28, 2000).

characteristics found in GAO's cost estimating and assessment guide.⁴⁶ OMB further questioned the reliability of these estimates because they believed staff other than the CIO had completed the survey and were therefore not experienced enough to provide knowledgeable estimates.

We disagree with OMB's opinion regarding the validity of our survey results for the following reasons. First, in meetings with CIOs and selected senior officials from agencies in our review to discuss our plans to survey the CIOs, we consistently expressed our expectation that the CIOs were to complete the survey. If this was not feasible, CIOs could delegate it to other staff, especially when agencies wanted staff that worked directly on addressing the reporting requirements to complete the survey because they were best qualified to respond to our questions. In these cases, we nevertheless told the agencies the CIOs were ultimately responsible for reviewing the accuracy of the survey results.

Second, we pretested the survey at seven agencies, again reinforcing our expectation that CIOs were to complete the survey. Specifically, to minimize errors that might occur from respondents interpreting our questions differently from our intended purpose, we pretested the questionnaire in person and by phone in three rounds of testing with officials from the office of the CIO at seven agencies. The selection of agencies for pretesting was based on agency availability to assist us with pretesting, variation in size of agency, and variation in agency CIO models (i.e., centralized or decentralized). During these pretests, we asked agency officials to complete the questionnaire for one reporting requirement as we listened to the process. We then interviewed the respondents to check whether the questions were applicable, clear, unambiguous, and easy to understand.

Third, in transmitting the surveys to the CIOs, we sent them directly to each of the 24 agency CIOs with instructions indicating that they were to complete it, with assistance from other officials as appropriate, and that the results would be summarized in a report to our congressional requesters. Specifically, in coordination with GAO survey methodology experts, we developed and administered a web-based survey that we sent to the CIOs of the 24 CFO Act agencies. All 24 CFO Act agencies completed the final survey. We then reviewed all responses, and followed up by phone and e-mail to clarify the responses as appropriate.

⁴⁶GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP(Washington, D.C.: March 2009).

The above three points notwithstanding, we have revised the report to note that CIO responses may have in some cases, come from agency officials completing the surveys on behalf of the CIOs.

In terms of the estimated costs of meeting reporting requirements, the application of GAO's cost guide in this context would be inappropriate, according to an internal GAO subject matter expert who co-authored the guide. This expert said the guide is reserved for the evaluation of government acquisition program cost estimates. The expert added that given that GAO was not reviewing such programs in this case, OMB's assertion is without merit. In addition, we initially asked OMB whether it had cost information on the reporting requirements but was told it did not and were directed to the 24 agencies as the best source. Further, we believe that we have appropriately qualified the range of costs reported by the agencies and note that we made no recommendations on the cost of such reporting.

Further, regarding OMB's comment about the experience of the staff providing estimates, we expressed our expectation that the CIOs complete this and the other parts of our survey. However, as previously discussed, in some cases CIOs and selected staff from the 24 agencies delegated this responsibility to agency subject matter experts who they thought were more knowledgeable in this area. In these cases, we again expressed our expectation that the CIOs at a minimum review the accuracy of such estimates.

With regard to the OMB concern about our report's contextual framing of certain information related to its efforts, the agency stated that it appreciated our draft report acknowledging that agency reporting is a critical component of ensuring effective management and oversight of key IT reform initiatives and that such information is essential to the success of IT reform efforts; however, it said our draft lacked contextual framing because it did not fully address the value of the reporting requirements beyond agency CIOs' use of the data. In particular, OMB stated that these requirements helped ensure the successful implementation of federal law and/or supported administration priorities, including IT-related cross-agency priority goals (which OMB commonly

refers to as CAP goals⁴⁷). According to OMB's comments, CAP goals cover areas—specifically, cybersecurity, Open Data, and smarter IT delivery—in which increased cross-agency collaboration is needed to improve progress towards shared, complex priorities reaching far beyond the scope of the priorities of individual federal agencies.

We included a description in our report of the value of the information to OMB in carrying out federal laws and its statutory roles and responsibilities. Specifically, consistent with OMB's comments, we point out that OMB utilizes reported information to meet statutory responsibilities. For example, our draft states that under federal law, OMB's Office of E-Government and Information Technology is required to submit a report on the implementation of the E-Government Act of 2002, which summarizes information reported by agencies as required under the act. The draft also says that during the period of our review, OMB was required to submit a report on federal agencies' implementation of the Federal Information Security Management Act of 2002. Further, the draft notes that in order to prepare such reports, OMB requires agencies to submit information on their implementation efforts as required under the acts, which OMB then summarizes for Congress.

Our report also discusses the administration's priorities such as the IT-related cross-agency priority goals. OMB's written comments acknowledge this point by stating that our draft report mentions the CAP goals. However, OMB notes that our draft does not provide essential context as to how the goals relate to reporting requirements. We disagree. Our draft stated that the CIO reporting requirements help the Federal CIO in its efforts to meet the CAP goals. Specifically, the draft noted that Office of E-Government and Information Technology officials review existing requirements to identify potential changes, including opportunities to streamline, when new government-wide IT initiatives are introduced. For example, these officials reported that their office is currently in the process of evaluating CIO and other reporting requirements to determine how they align to OMB's strategic cross-agency priority goals associated with smarter IT delivery, cybersecurity,

⁴⁷As noted earlier, the GPRA Modernization Act of 2010 required OMB to establish cross-agency priority goals to address longstanding challenges where implementation required active collaboration between multiple agencies in order to improve progress. Three goals related to federal IT management were established: smarter IT delivery, Open Data, and cybersecurity.

and Open Data and whether there might be opportunities to further streamline existing reporting requirements

Regarding OMB's fourth concern that our report does not reflect steps it has taken to solicit feedback and streamline requirements, the agency commented that it holds quarterly review (feedback) sessions with agency officials about IDC requirements. It added that these sessions have resulted in streamlining OMB collection requirements. OMB also noted that it meets with CIO council members (via a Federal Data Center Consolidation Initiative task force) to, among other things, help develop metric and data collection requirements that best support administration goals in this area. According to OMB, it has changed reporting requirements and its strategic approach with regard to the data center initiative as a result of feedback from the task force. In addition, OMB cited the annual capital planning and investment control guidance it issues, which includes Exhibits 53 and 300 reporting requirements, as another example of the agency soliciting feedback.

The streamlining efforts described in OMB's comments are discussed in our report, including the role OMB played in soliciting of feedback. For this reason, we agree with and believe our draft is consistent with OMB's comments as it relates to IDC requirements and the annual capital and control guidance it issues. Regarding its data center consolidation efforts, we are aware of this effort and have updated our report to show it as another example of OMB's efforts to streamline and solicit feedback. Nonetheless, OMB's comments provided no explanation or documentation to show it was addressing the CIO-identified challenges in our draft that are not currently being addressed by its streamlining efforts.

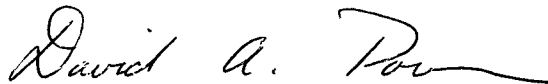
The above efforts aside, agency CIOs suggested, as noted in our report, that OMB's feedback process could nonetheless be improved. In particular, while agency CIOs reported that OMB provided feedback to them on the majority of the 36 reporting requirements, the majority of CIOs reported that the feedback was moderately effective to not effective for most reporting requirements. Six agency CIOs also reported that they were specifically interested in receiving better feedback on two reporting requirements—namely, the major IT investment documentation and the Open Government directive. Office of E-Government and Information Technology officials stated that the information on the feedback, particularly those requirements agency CIOs were interested in receiving feedback on, was useful.

Nevertheless, the officials acknowledged that they do not consistently provide this level of feedback to the CIOs because, in part, they did not

know until now that the CIOs wanted feedback to this extent. Having a process that consistently provides effective feedback is key to helping agency CIOs better manage their IT resources and improve reporting; it is also consistent with OMB's goals to improve federal IT management, oversight, and transparency. Until an effective feedback process is in place, there is a risk that agencies are managing their IT in a suboptimal manner.

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 is available at no charge on GAO's website at <http://www.gao.gov>.

If you or your staffs have any questions on the matters discussed in this report, please contact me at (202) 512-9286 or pownerd@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 V.



David A. Powner
Director, Information Technology
Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) identify the current information technology (IT) reporting requirements that agency chief information officers (CIO) are to address for the Office of Management and Budget (OMB); (2) evaluate the extent to which OMB and agency CIOs use the required information to manage IT, including CIOs' views on the utility of the requirements; and (3) assess any OMB efforts to streamline this reporting.

To identify the current CIO IT management reporting requirements, we obtained and analyzed OMB circulars, memorandums, and other issued guidance to develop a current list of requirements to report information to OMB; the resulting list included regular, recurring, or one-time requirements that were in effect as of March 2014. We focused on the requirements that were in effect by the end of the second quarter in fiscal year 2014 (i.e., March 2014) so that we could use these in our survey of federal agency CIOs, which was issued in May 2014.¹ In addition, since there could be several requirements for information in multiple OMB memorandums for one initiative, we grouped the requirements to report information together by initiative and the frequency of reporting rather than list each as its own separate requirement. Requirements related to activities such as information collection and control of paperwork; records management; privacy and compliance with the Privacy Act; and information disclosure and compliance with the Freedom of Information Act were not included because these activities are not directly related to IT management responsibilities. Further, requirements directed to other agency officials but to which the agency CIO contributes were not included. Further, although OMB occasionally makes ad hoc requests to agency CIOs to provide information, we did not include those items in our list because they did not originate from issued guidance.

We categorized the requirements based on their best fit in the following areas that are typically identified as key CIO IT management responsibilities: IT strategic planning; capital planning and investment management; IT security; and system acquisition, development, and integration. We also had the agencies in our review (the 24 Chief

¹Following the conclusion of our survey, we learned from OMB that two requirements we had listed in our survey were no longer in effect. Therefore, we eliminated two requirements from our list and determined that we would not include the survey responses related to those requirements in our report.

Financial Officer (CFO) Act agencies²) and OMB review our list and provide feedback to help ensure it was complete and accurate. Based on their feedback, we made the necessary changes to our list, including adding several requirements and removing several requirements that were no longer in effect.

To evaluate the extent to which agency CIOs and OMB use the required information to manage IT and to assess CIOs' views on the utility of the requirements, we first obtained and analyzed OMB documentation and interviewed OMB officials; we then compared it to OMB's goal of using CIO-reported information to improve the management, oversight, and transparency of federal IT. We also, in coordination with our survey methodology expert, developed and administered a web-based survey that we sent to the CIOs of the 24 CFO Act agencies. In meetings with CIOs and selected senior officials from agencies in our review to discuss our plans to survey the CIOs, we told them we expected the CIOs to complete the survey. If this was not feasible, CIOs could delegate the task to other staff, especially when agencies wanted staff that worked directly on addressing the reporting requirements to complete the survey because they were best qualified to respond to our questions. In these cases, we nevertheless told the agencies the CIOs were ultimately responsible for reviewing the accuracy of the survey results.

Using the survey, we requested information on, among other things, the usefulness of the reporting requirements in managing IT, the level of effort required to meet them, and whether CIOs thought the requirements should be changed. For our analysis and reporting of the questions on usefulness and level of effort, we grouped the reported responses into three categories (i.e., very great to great, moderate, and some to no extent) and reported the category that had a majority response, or the largest number of responses in cases where the total number of respondents for a particular requirement was less than 24. In instances where the number of responses was evenly, or close to evenly, divided between the "very great to great" and "some to no extent" categories, we

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

chose the moderate category, as it provided the best overall representation of the views of the agency CIOs for that requirement. For the question on proposed changes to the reporting requirements, we provided six options of possible change for agency CIOs to choose from for each reporting requirement (i.e., frequency, mechanism, information provided, consolidation, elimination, or other). We determined that at least eight responses or one third of respondents suggesting a particular change represented a sufficient consensus of agency CIO views for reporting purposes.

In addition, for each requirement, we asked agency CIOs to estimate the annual amount (in government and/or contractor dollars) that agencies spent on meeting each reporting requirement. For each reporting requirement, we provided four choices in the survey to choose from (\$1-\$99,000; \$100,000-\$299,000; \$300,000-\$1,000,000; and more than \$1,000,000). We decided not to offer more precise dollar amount options to choose from because, among other things, agencies do not typically keep track of funds spent on CIO reporting requirements because this is not required by OMB and therefore the benefits of having more precise amounts were outweighed by the time and effort agencies would have had to expend to develop such precise estimates. For our analysis of how much agencies spend annually on reporting requirements, since the option "more than \$1,000,000" did not include an upper range, we worked with a survey methodology expert to define the lower and upper range of this choice to be the same, which is \$1 million plus one dollar or \$1,000,001. See appendix III for the list of survey questions.

To minimize errors that might occur from respondents interpreting our questions differently from our intended purpose, we pretested the questionnaire in person and by phone in three rounds of testing with officials from the office of the CIO at seven agencies. The selection of agencies for pretesting was based on agency availability to assist us with pretesting, variation in size of agency, and variation in agency CIO models (i.e., centralized or decentralized). During these pretests, we asked agency officials to complete the questionnaire for one reporting requirement as we listened to the process. We then interviewed the respondents to check whether the questions were applicable, clear, unambiguous, and easy to understand. All 24 CFO Act agencies completed the final survey, although not all survey respondents answered every question. We then reviewed all responses, and followed up by phone and e-mail to clarify the responses as appropriate.

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

To assess any OMB efforts to streamline this reporting, we obtained and analyzed OMB and Federal CIO Council documentation and interview information to summarize OMB's current and future plans for streamlining CIO reporting and compared these efforts with OMB's goal to reduce CIO reporting burden. As part of this, we interviewed officials from OMB and the Federal CIO's Capital Planning and Investment Control Community of Practice key working group to identify current and future actions taken to streamline CIO reporting requirements.

We conducted this performance audit from December 2013 to April 2015 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 base on our audit objectives.

Appendix II: Chief Information Officer IT Management Reporting Requirements

The following table lists the 36 OMB requirements for agency Chief Information Officer reporting on IT management, along with the source of requirement and the year that the requirement was established.

Table 5: Chief Information Officer Reporting Requirements, including Source and Year Established

Reporting requirement	Source(s)	Year established
1. Information Resources Management strategic plan	OMB, Management of Federal Information Resources, Circular A-130 OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	1996
2. Enterprise roadmap	OMB Memorandum, Increasing Shared Approaches to Information Technology Services	2012
3. Exhibit 53	OMB, Preparation, Submission, and Execution of the Budget, Circular A-11 OMB, Fiscal Year 2015 Guidance on Exhibits 53 and 300 – Information Technology and E-Government	1999 ^a
4. Exhibit 300	OMB, Preparation, Submission, and Execution of the Budget, Circular A-11 OMB, Fiscal Year 2015 Guidance on Exhibits 53 and 300 – Information Technology and E-Government	1998 ^a
5. Major IT investment documentation	OMB, Fiscal Year 2015 Guidance on Exhibits 53 and 300 -Information Technology and E-Government	2013
6.IT capital plan	OMB, Management of Federal Information Resources, Circular A-130	2000
7. PortfolioStat progress report	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
8. PortfolioStat review	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
9. Compliance failures	OMB, Management of Federal Information Resources, Circular A-130	2000
10. IT security key metrics	OMB, Quarterly E-Gov Integrated Data Collection Guidance	2013
11. Cybersecurity performance improvements	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
12. Federal Risk and Authorization Management Program key metrics	OMB Memorandum, Security Authorization of Information Systems in Cloud Computing Environments	2011
13. Government-wide tracking of resources for cyber activities	OMB, Budget Data Request, Government-wide Tracking of Resources for Cyber Activities	2012
14. Information security continuous monitoring dashboard	OMB, Enhancing the Security of Federal Information and Information Systems, M-14-03	2013
15. Monthly IT security data feeds	OMB, Fiscal Year 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-11-33	2011
16. IT security quarterly reporting	OMB, Fiscal Year 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-10-15	2010
17. Annual Federal Information Security Management Act report	OMB, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, M-03-19 ^{a,b}	2003 ^a

**Appendix II: Chief Information Officer IT
Management Reporting Requirements**

Reporting requirement	Source(s)	Year established
18. Cybersecurity plan of action	OMB, Fiscal Year 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-12-20	2012
19. Personal Identity Verification credentials report (Homeland Security Presidential Directive 12)	OMB, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials, M-07-06 OMB, Homeland Security Presidential Directive 12 Implementation Status, M-08-01	2007
20. Trusted Internet Connections initiative	OMB, Update on the Trusted Internet Connections Initiative, M-09-32	2009
21. Report significant IT security deficiencies	OMB, Management's Responsibility for Internal Control, Circular A-123	2004
22. Cost savings/avoidances	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
23. IT investment baseline updates	OMB, Information Technology Investment Baseline Management Policy, M-10-27	2010
24. IT investment performance updates	OMB, Information Technology Investment Baseline Management Policy, M-10-27	2010
25. Agency TechStat outcomes	OMB, Quarterly E-Gov Integrated Data Collection Guidance	2013
26. Cloud First	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
27. Commodity IT baseline update	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
28. Mobile contracts inventory update	OMB, Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management, M-13-09	2013
29. Data center closures/status update	OMB Memorandum, Implementation Guidance for the Federal Data Center Consolidation Initiative, March 29, 2012	2012
30. E-Government status report	OMB, Implementation Guidance for the E-Government Act of 2002, M-03-18 ^a	2003
31. Open Government directive	OMB, Open Government Directive, M-10-06	2009
32. Open data policy enterprise inventory	OMB, Open Data Policy-Managing Information as an Asset, M-13-13	2013
33. Open data policy public data listing	OMB, Open Data Policy-Managing Information as an Asset, M-13-13	2013
34. Open data policy customer feedback process	OMB, Open Data Policy-Managing Information as an Asset, M-13-13	2013
35. Open data policy data publication process	OMB, Open Data Policy-Managing Information as an Asset, M-13-13	2013
36. Agency points of contact	OMB, Quarterly E-Gov Integrated Data Collection Guidance	2013

Source: GAO analysis. | GAO-15-106

^aOMB releases annual guidance for how agencies are to meet these requirements, which can include significant changes to the requirement.

^bAlthough OMB has incorporated agency reporting on privacy-related issues into annual Federal Information Security Management Act reporting, we have not included privacy since it was considered outside the scope of our work. See app. I for more details.

Appendix III: Survey of Federal Agency Chief Information Officers

The following is an abridged version of the CIO reporting requirements survey. This version includes the set of questions for one requirement, which was repeated for each of the requirements in our survey.



United States Government Accountability Office

Chief Information Officer (CIO) Reporting Requirements Survey

Introduction

At the request of the Senate Committee on Homeland Security and Governmental Affairs, GAO is reviewing current information technology (IT) reporting requirements that the Office of Management and Budget (OMB) requires agency Chief Information Officers (CIO) to address. As part of this review, GAO is conducting a web-based survey of the 24 Chief Financial Officers (CFO) Act federal agencies to collect information about the utility of these CIO reporting requirements. The focus of this review is to evaluate the utility of the reporting requirements and your answers are not being evaluated.

This survey should be completed by the agency CIO, although GAO acknowledges that the CIO may need to consult other agency officials, such as the CFO or Chief Operations Officer and component/bureau CIOs, who are familiar with these reporting requirements to help provide complete responses.

If you want to review the entire survey or distribute the entire survey or selected sections to others in your agency before completing it online, you may download an Adobe Acrobat read only copy. This copy contains a table of contents on page 2 showing the pages in the Adobe Acrobat version containing the questions we are asking for each of the 38 CIO reporting requirements.

You may also download an Adobe Acrobat copy of the 38 CIO reporting requirements covered in the survey showing the source of the requirement, a description of the requirement, and the frequency of reporting.

Your answers will be combined with those from the other CFO Act agencies and will be summarized in a report to Congress. GAO may also include illustrative examples of statements provided. However, GAO will not attribute responses or examples to individual agencies or release individually identifiable agency data from this survey unless specifically requested by Congress or compelled by law.

GAO understands that there are great demands on your time; however, your response is crucial in helping provide important information to Congress.

Thank you in advance for your cooperation.

**Appendix III: Survey of Federal Agency Chief
Information Officers**

Contact Information

While we realize that a number of individuals at your agency will be providing answers for the specific reporting requirements, we ask that a single individual incorporate the answers received from the various participants and complete the Web-based questionnaire. Please provide the following information for the primary person completing this questionnaire in the event we need to clarify a response.

Name:

Title:

Department/agency:

Name of office or unit:

E-mail:

Telephone:

Questions for the 38 CIO Reporting Requirements

Note: The following set of questions was repeated for each of the 38 CIO reporting requirements included in GAO's survey. The following information was provided for each of the reporting requirements.

Requirement Category: e.g., IT Strategic Planning/IT Workforce Planning

Source of Requirement: e.g., A-130/M-13-09/44 U.S.C. 3506 (b)(2)

Name and Description of the Requirement: e.g., Information Resource Management (IRM)
Strategic Plan: Agencies must develop and maintain an IRM Strategic Plan. An IRM Strategic Plan describes how the agency is applying information resources to improve the productivity, efficiency, and effectiveness of government programs.

Frequency of Reporting: e.g., Annually

1. To what extent, if at all, does addressing the above requirement assist your agency in managing IT?

- ☐ Very great extent
☐ Great extent
☐ Moderate extent
☐ Some extent
☐ No extent

1a. Please explain why you selected that response.

2. What level of effort is required by your agency to meet the reporting requirement?

- ☐ Very great effort
☐ Great effort
☐ Moderate effort
☐ Some effort
☐ Little or no effort

3. To address this reporting requirement, does your agency do the following?
(Select one answer in each row.)

	Yes	No
a. Create a new document	<input type="checkbox"/>	<input type="checkbox"/>
b. Modify an existing agency document	<input type="checkbox"/>	<input type="checkbox"/>
c. Conduct a data call to obtain required information	<input type="checkbox"/>	<input type="checkbox"/>
d. Analyze and summarize agency data	<input type="checkbox"/>	<input type="checkbox"/>
e. Format or convert agency data into an OMB-required format (e.g., MAX Portal, Integrated Data Collection, CyberScope, etc.)	<input type="checkbox"/>	<input type="checkbox"/>
f. Other	<input type="checkbox"/>	<input type="checkbox"/>

(If other) Please specify what else your agency
does to address this reporting requirement.

--

4. Using your best estimate, approximately how much does your agency spend (in terms of
government and/or contract dollars) on an annual basis to meet the reporting requirement?

(Please note: Your response to this question will be aggregated and agencies will not be identified
individually.)

- ☐ \$1 - \$99,999
☐ \$100,000 - \$299,999
☐ \$300,000 - \$1,000,000
☐ More than \$1,000,000

5. For this requirement, has your agency received feedback within the past 12 months from OMB or
a designated partner agency (e.g., feedback from the Department of Homeland Security regarding
requirements regarding cybersecurity)?

- ☐ Yes
☐ No

- (If yes) How effective, if at all, has this feedback been to help improve your agency's ability to manage its IT?

- ☐ Very effective
- ☐ Effective
- ☐ Moderately effective
- ☐ Slightly effective
- ☐ Not effective

- (If no) Would your agency find it useful to receive feedback from OMB or designee?

- ☐ Yes
- ☐ No
-
- ☐ No opinion

6. In your opinion, should this requirement be changed in any of the following ways?
(Select all that apply.)

- ☐ No change is needed
-
- ☐ Change the frequency of reporting
- ☐ Change the mechanism of reporting (i.e., MAX Portal, Cyberscope, e-mail)
- ☐ Modify the requirement (i.e., change what information is reported)
- ☐ Consolidate or combine with other requirements
- ☐ Eliminate the requirement
- ☐ Other

- Currently, the reporting frequency of this requirement is (frequency of requirement was populated here). If you selected "Change the frequency of reporting," what frequency do you think the level of reporting should be?

- ☐ Monthly
- ☐ Quarterly
- ☐ Semi-annually
- ☐ Annually
- ☐ Biennial
- ☐ Other - (If other) What should the frequency of reporting be?

- If you selected "Change the mechanism of reporting," please specify why the mechanism should be changed and what the mechanism should be.

- If you selected "Modify the requirement," please specify how the requirement should be modified.

- If you selected "Consolidate or combine with other requirements," please specify with what other requirement(s) it should be consolidated or combined.

- If you selected "Eliminate the requirement," please specify why it should be eliminated.

- If you selected "Other," please specify what other change to the requirement you would recommend.

7. If this was not a specific reporting requirement, would your agency still collect all, most, some, or none of the information contained in the requirement in order to manage its IT?

- ☐ All
☐ Most
☐ Some
☐ None

7a. (Optional) Please explain your answer.

Duplication and Overlap Questions

Please note: The questions in this section focus on all of the CIO reporting requirements covered in this survey. We would like the opinions of agency CIOs on whether there is duplication or overlap in the data requested by OMB pertaining to the CIO reporting requirements that creates an unnecessary burden on federal agencies

1. In your opinion, is there duplication and/or overlap in the data requested by OMB pertaining to the CIO reporting requirements that GAO has included in this survey that created an unnecessary burden on your agency?

☐ Yes

☐ No

☐ No opinion/No basis to judge

- 1a. (If yes) Please describe the reporting requirements and the specific information that is duplicative or overlapping.

- 1b. For those reporting requirements described in question 1a, which reporting requirement(s), if any, should be eliminated or consolidated with other requirement(s)?

Survey Completion Question

Are you ready to submit your final completed survey to GAO?

(This is equivalent to mailing a completed paper survey to us. It tells us that your answers are official and final.)

☐ Yes, my survey is complete

☐ No, My survey is not yet complete

Thank you very much for your assistance.

Appendix IV: Comments from the Office of Management and Budget



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

March 23, 2015

Mr. David A. Powner
Director
IT Acquisition Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Powner:

Thank you for providing the Office of Management and Budget (OMB) the opportunity to review and provide comments on a draft of GAO's report on "Federal Chief Information Officers: Reporting to OMB Can Be Improved By Further Streamlining and Better Focusing on Priorities" (GAO-15-106).

We appreciate the time and energy that GAO has devoted to reviewing agency Chief Information Officer (CIO) reporting requirements, agency views on the usefulness of these requirements in managing Information Technology (IT), and OMB's efforts to streamline these requirements.

While we acknowledge the importance of effectively reviewing and communicating reporting requirements, we have concerns regarding the report's accuracy in counting requirements, approach for certain aspects of the survey, and contextual framing. Specifically, our primary concerns are that:

- The report's count of CIO reporting requirements is not currently accurate;
- The survey approach does not fully support the findings and conclusions;
- The objective to solicit "CIOs' views" does not allow for sufficient contextual framing; and
- OMB has taken steps to solicit feedback and streamline requirements not reflected in the report.

Thus, we must respectfully neither agree nor disagree with the recommendations. Although we have chosen to take no position on the recommendations due to these concerns, we do agree with the principles contained in the recommendations that stress the importance of a common understanding with CIOs and other key stakeholders on the importance and priority of reporting requirements, ensuring effective and constructive feedback to CIOs on reported information, and streamlining reporting requirements. We have actively incorporated these principles into our work, as discussed below, and continuously work to enhance our efforts in these areas.

The Report's Count of CIO Reporting Requirements Is Not Currently Accurate

The draft report states that agencies must address 36 IT management reporting requirements to OMB; however, at least seven of these requirements: (1) did not exist as OMB requirements at the time of the GAO audit, (2) were eliminated during or shortly after the audit timeframe, or (3) appear to have been double-counted.

1. Two items did not exist as OMB requirements at the time of the GAO audit and do not currently exist as OMB requirements:
 - OMB did not require the Information Security Continuous Monitoring (ISCM) dashboard, which does not yet exist and will be implemented as part of the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program in

- fiscal year (FY) 2016. This automated dashboard will replace or streamline multiple manual reporting requirements that currently exist.
- OMB did not and does not require agencies to provide cybersecurity plans of action.
2. OMB eliminated two requirements during or shortly after the audit timeframe.
- “PortfolioStat review,” (not to be confused with the actual PortfolioStat sessions) as noted by the draft report, was a one-time reporting requirement to solicit feedback about the PortfolioStat process and reporting requirements.
 - The Commodity IT baseline update was eliminated in May 2014, as acknowledged by the draft GAO report, in response to feedback from agency CIOs.
3. GAO appears to have double-counted three requirements, which are actually components of other counted requirements.
- The IT capital plan and Cloud First are components of the already-listed Exhibit 53.
 - The “open data policy public data listing” is a subset of the “open data enterprise inventory.” Agencies simply need to copy-and-paste this subset into a new file and put it on their website to fulfill the requirement.

The Survey Approach Does Not Fully Support the Report’s Findings and Conclusions

The Draft Report Attributes Views to CIOs; However, Many CIOs May Not Have Personally Provided Survey Input

The draft report states that GAO conducted a survey of 24 major agency CIOs and broadly attributes views and opinions to agency CIOs over 50 times. However, we do not believe such high-level attribution is appropriate because the agency CIO may not have personally taken the survey. Many agency CIOs who served during the GAO audit period stated to OMB, through the CIO Council, that they delegated full responsibility for completing the survey to lower-level staff. Some other agency CIOs reported that they could not recall that a survey was conducted.

Additionally, the survey (as presented in the report appendix) envisions responses from non-CIO agency personnel. This is because the survey states that CIOs “should” complete the survey, but acknowledges that “a number of individuals at your agency will be providing answers for the specific reporting requirements.” Thus, agency CIOs may have had little to no direct input into the responses. Since the survey results underlie much of the report, we do not have full confidence in some of the report’s findings.

Survey-Derived Cost Estimates Are Given Disproportionate Weight Relative to Methodological Approach

The draft report uses survey responses to estimate that agencies spend \$150 million to \$308 million each year on OMB’s reporting requirements. GAO cites these estimates multiple times in the report, including to support GAO’s conclusions that OMB’s reporting requirements constitute an “annual multi-hundred million dollar financial commitment.”

These estimates appear unsubstantiated, so we do not believe that they warrant the weight GAO gives them. GAO published an estimation guide¹ that highlighted nine basic characteristics of a credible cost

¹ *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

estimate, yet all of GAO's cost estimates for OMB's reporting requirements come from a single survey question (reprinted below) that does not require any of these basic characteristics. The draft report's methodology appendix goes on to state that "agencies do not typically keep track of funds spent on CIO reporting requirements." Further, we have found no evidence in GAO's report that the lower-level staff who completed a number of these surveys are organizationally well-positioned and experienced enough to provide knowledgeable estimates of the cost of reporting requirements. For these reasons, we do not believe costs estimated in the report are reliable.

Using your best estimate, approximately how much does your agency spend (in terms of government and/or contract dollars) **on an annual basis** to meet the reporting requirement?

(Please note: Your response to this question will be aggregated and agencies will not be identified individually.)

- ☐ \$1 - \$99,999
- ☐ \$100,000 - \$299,999
- ☐ \$300,000 - \$1,000,000
- ☐ More than \$1,000,000

The Objective to Solicit "CIOs' Views" Does Not Allow For Sufficient Contextual Framing

OMB appreciates GAO's acknowledgement, both through the draft and prior GAO reports, that OMB's IT reform efforts are key to improving the efficiency and effectiveness of Federal agency programs and operations. OMB also appreciates GAO's acknowledgement that a critical component of ensuring effective management and oversight of these key IT reform initiatives is through agency reporting in response to OMB's requirements and that such information is essential to the success of IT reform efforts. However, the draft report's second objective, to "evaluate the extent to which OMB and agency CIOs use the required information to manage IT, including CIOs' views on the utility of the requirements," lacks contextual framing because it does not fully address the value of reporting requirements beyond agency CIOs' use of the data. Moreover, framing the objective around CIOs' opinions of such reports results in an incomplete discussion of the value of these requirements for other priorities and stakeholders.

At least nine of these reporting requirements help ensure the successful implementation of Federal law.² Some of OMB's legislative reporting requirements may surpass the minimum legal requirements; however, we are confident that the additional information collected is critical to ensure the successful implementation of the law and the successful management of Federal IT.

² The reporting requirements are Exhibit 300, Exhibit 53, Annual Federal Information Security Management Act (FISMA) Report, Report significant IT security deficiencies, IT investment baseline updates, IT investment performance updates, Cost savings/avoidances, Data center closures/status update, and the E-Government status report. These reporting requirements help implement a number of laws, including the Clinger-Cohen Act, Federal Information Technology and Reform Act (FITARA), Federal Information Security Modernization Act (FISMA) of 2014, Federal Managers' Financial Integrity Act (FMFIA) of 1982, Financial Services and General Government (FSGG) Appropriations for FY2012-2015, and the E-Government Act of 2002.

Additionally, at least 11 of the reporting requirements support Administration priorities, including IT-related Cross-Agency Priority (CAP) goals. These CAP goals have been implemented as part of the GPRA Modernization Act of 2011, which requires OMB to coordinate with agencies to establish outcome-oriented, cross-cutting Federal government goals, and to provide quarterly reports on the progress of these goals.³ The Federal CIO plays a significant leadership role in reaching the Cybersecurity, Open Data, and Smarter IT Delivery CAP goals, each of which involves reporting requirements to implement CAP goal initiatives and/or track progress. Although the draft report mentions the CAP goals, it does not provide essential context as to how the goals are related to reporting requirements. The reporting requirements and associated CAP goals are listed below:

CAP Goal Title	Goal Statement	Associated Reporting Requirements
Cybersecurity	Improve awareness of security practices, vulnerabilities, and threats to the operating environment, by limiting access to only authorized users and implementing technologies and processes that reduce the risk from malicious activity.	<ul style="list-style-type: none"> • Cybersecurity performance improvements • Monthly IT security data feeds • IT security quarterly reporting • FISMA report • Trusted Internet Connections initiative
Open Data	Fuel entrepreneurship and innovation, and improve government efficiency and effectiveness by unlocking the value of government data and adopting management approaches that promote interoperability and openness of data	<ul style="list-style-type: none"> • Open data policy enterprise inventory • Open data policy public data listing • Open data policy customer feedback process • Open data policy data publication process
Smarter IT Delivery	Eliminate barriers and create new incentives to enable the Federal Government to procure, build, and provide world-class, cost-effective IT delivery for its citizens	<ul style="list-style-type: none"> • Exhibit 53 • Exhibit 300

CAP goals cover areas in which increased cross-agency collaboration is needed to improve progress towards shared, complex priorities reaching far beyond the scope of the priorities of individual Federal agencies. Given this complexity, assessing the usefulness of such efforts by referencing the opinions of CIOs or their staff in the context of reporting requirements does not adequately assess the value of the reporting requirements associated with these goals. Cybersecurity is critical in protecting Federal networks and the privacy of American citizens, Open Data has the potential to fuel innovation and unlock billions of dollars in economic benefits,⁴ and Smarter IT Delivery can transform the way government serves its citizens through digital services. Each of these objectives exists for a purpose beyond the interests of any one stakeholder or group.

³ See <http://www.performance.gov> for these reports and additional information on CAP goals.

⁴http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information

OMB Has Taken Steps to Solicit Feedback and Streamline Requirements Not Reflected In the Report

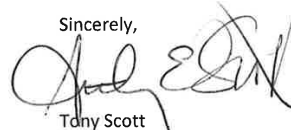
OMB greatly values agency feedback on our reporting requirements to support effective oversight and reform efforts and regularly solicits and incorporates feedback from CIOs and other agency officials to enhance the value of our reporting requirements. To this end, we hold open quarterly review sessions with agency officials about Integrated Data Collection (IDC) requirements. These feedback sessions have resulted in significant streamlining of our collection requirements, including the elimination of the commodity IT baseline update reporting requirement, which GAO cited as having “some to no usefulness and very great effort.” The draft report recognizes the elimination of this requirement; however, it does not acknowledge that the change resulted from agency feedback.

Another example of OMB engaging the CIO community to improve the value of agency reporting is the Federal Data Center Consolidation Initiative (FDCCI). To ensure that the reporting requirements related to FDCCI are capturing the data that agency CIOs feel is most important, the OMB-chaired CIO Council convenes a committee of agency officials, known as the FDCCI Task Force, to help develop the metrics and data collection requirements that best support the Administration goals of consolidating and optimizing data centers. As a result of feedback from the FDCCI Task Force, OMB has made significant changes to both its reporting requirements and strategic approach, illustrating both the value of the group’s contributions and OMB’s desire to work with agencies to achieve mutual goals. Although agency officials designed many of the metrics and reporting requirements themselves and agencies have reported that FDCCI has the potential to save them over \$5 billion in saving over the next few years⁵, GAO’s draft report states that agencies find “little to no” usefulness in the data center reporting requirement. These inconsistencies raise additional concerns for us regarding the survey results, as discussed above.

Finally, OMB’s annual Capital Planning and Investment Control (CPIC) guidance, which provides the reporting requirements for Exhibit 53 and Exhibit 300, undergoes an extensive interagency comment and vetting period prior to being issued. Additionally, for the last several years, the process of determining the extent to which reporting requirements should be added, modified, or removed has been led by an agency official assigned to OMB, often from a CIO Council committee.

Thank you again for providing OMB the opportunity to submit comments on the draft. Although we take no official position on the recommendations, we remain committed to continuously improving our data collection efforts and the usefulness of the information collected to a wide range of stakeholders. Despite our views on this particular report, we look forward to our continued partnership in enhancing the management of Federal IT and welcome the opportunity to further develop relationships with you and your dedicated staff.

Sincerely,



Tony Scott
U.S. Chief Information Officer
Office of Management and Budget

⁵ GAO, *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings*, [GAO-14-713](#) (Washington, D.C.: Sept. 25, 2014).

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner, (202) 512-9286, or pownerd@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff made key contributions to this report: Gary Mountjoy (Assistant Director); Scott Borre; Chris Businsky; Valerie Hopkins; Stuart Kaufman; Lee McCracken; Tarunkant Mithani; and Teresa Smith.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

E-mail: fraudnet@gao.gov

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

Congressional Relations

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

Public Affairs

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

