



---

April 2017

Highlights of a Forum

# Information Technology

## Opportunities for Improving Acquisitions and Operations

Convened by the Comptroller General of the United  
States

Accessible Version

# GAO Highlights

Highlights of [GAO-17-251SP](#), a GAO forum

## Why GAO Convened This Forum

IT expenditures too often have produced failed projects—that is, projects with multimillion dollar cost overruns and schedule delays measured in years, with questionable mission-related achievements and duplicative and inefficient operational systems. In December 2014, IT reform legislation was enacted which requires agencies to address key IT issue areas. To help address these ongoing challenges, GAO recently added improving the management of IT acquisitions and operations to its list of high-risk areas for the federal government.

While GAO has made over 800 recommendations aimed at improving IT acquisitions and operations outcomes, slightly less than half of these recommendations have been fully implemented. In light of this, GAO assembled a panel of IT experts on September 14, 2016 to elicit additional ideas to further improve delivery and operations of IT.

The viewpoints summarized in the report do not necessarily represent the views of all participants, their organizations, or GAO. GAO provided participants the opportunity to review a summary of key points from the forum and incorporated their comments as appropriate prior to publishing this report.

View [GAO-17-251SP](#). For more information, contact David A. Powner at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov).

April 2017

## Information Technology

# Opportunities for Improving Acquisitions and Operations

## What the Participants Said

Forum participants discussed the challenges and opportunities for Chief Information Officers (CIO) to improve information technology (IT) acquisitions and operations—with the goal of better informing policymakers and government leadership. They identified key actions related to the following topics: strengthening the Federal Information Technology Acquisition Reform Act (FITARA), improving CIO authorities, budget formulation, governance, workforce, operations, and transition planning.

### STRENGTHENING FITARA'S IMPACT

- Congressional oversight could be more aggressive
- Office of Management and Budget (OMB) may need to strengthen its role
- The Department of Defense should be required to implement all provisions of FITARA

### IMPROVING CIO AUTHORITIES

- Have the Chief Information Officers Council play an enhanced role in improving authorities
- Implement collaborative governance
- Evolve the role of the CIO to enable change
- Focus on cybersecurity to change existing cultures

### BUDGET FORMULATION

- Use IT spend plans to improve budgets
- Examine agency programs to capture additional IT spending
- Simplify the definition of IT
- Work more closely with procurement organizations
- Work with congressional committees to explore budgeting flexibilities

### GOVERNANCE

- Obtain support from agency leadership
- Enhance governance at OMB and agencies
- Use security authorities to enhance governance
- Strengthen oversight for IT purchased as a service
- Buy more and develop less
- Evolve procurement processes to align with new technologies

### WORKFORCE

- Attract more qualified CIOs by appealing to key missions
- Have the Federal CIO play a more active role in attracting agency CIOs
- Give CIOs more human resource flexibilities
- Focus on attracting and investing in a more holistic IT workforce
- Better integrate private sector talent into the IT workforce

### OPERATIONS

- Use a strategic approach for legacy system migration
- Migrate more services to the cloud
- Implement strategies to mitigate the impact on jobs when closing data centers

### TRANSITION PLANNING

- Convey IT and cyber issues early to leadership
- Encourage Congress to focus on IT and cybersecurity at confirmation hearings
- Ensure that IT and cyber issues are OMB priorities
- Ensure GAO plays a role highlighting its work and expertise

Source: GAO analysis. | [GAO-17-251SP](#)

---

# Contents

---

Letter	1
Opportunities for Improving IT Acquisitions and Operations	4
Appendix I: Participants in the September 2016 Comptroller General Forum on IT Acquisitions and Operations	26
Appendix II: Forum Agenda	28
Appendix III: GAO Contact and Staff Acknowledgments	29
GAO Contact	29
Staff Acknowledgments	29

---

## Abbreviations

CIO	Chief Information Officer
IT	information technology
FITARA	Federal Information Technology Acquisition Reform Act
O&M	operations and maintenance
OMB	The 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 11, 2017

This report presents the results of a forum, convened by the Comptroller General on September 14, 2016, to explore challenges and opportunities for Chief Information Officers (CIO) to improve federal information technology (IT) acquisitions and operations—with the goal of better informing policymakers and government leadership.

The federal government annually invests more than \$80 billion on IT. Yet, these expenditures too often have produced failed projects—that is, projects with multimillion dollar cost overruns, schedule delays measured in years, and questionable mission-related achievements. Further, executive-level governance and oversight provided by CIOs has often been ineffective. We reported in 2011, for example, that not all CIOs had the authority to review and approve the management and operations of their agency’s IT investments and that CIOs’ authority was further limited in areas such as management of the IT workforce.<sup>1</sup>

Recognizing the severity of issues related to the government-wide management of IT, in December 2014, Congress enacted IT acquisition reform legislation (commonly referred to as the Federal Information Technology Acquisition Reform Act, or FITARA) as part of the Carl Levin and Howard P. ‘Buck’ McKeon National Defense Authorization Act for Fiscal Year 2015.<sup>2</sup> This law requires most major executive branch agencies to ensure that the CIO has a significant role in the decision-making process for IT budgeting, and in the management, governance, and oversight processes related to IT.<sup>3</sup> The law also required OMB to issue guidance requiring covered agency CIOs to, among other things, (1) approve the IT budget requests of their respective agencies, and (2) certify that investments are adequately implementing the Office of Management and Budget’s (OMB) incremental development guidance.<sup>4</sup> In addition, FITARA requires covered agency CIOs to (1) review and

---

<sup>1</sup>GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, [GAO-11-634](#) (Washington, D.C.: Sept. 15, 2011).

<sup>2</sup>Federal Information Technology Acquisition Reform provisions of the Carl Levin and Howard P. ‘Buck’ McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

<sup>3</sup>The Department of Defense is exempt from these provisions of the law.

<sup>4</sup>40 U.S.C. § 11319(b)(1)(B).

approve IT contracts, and (2) approve the appointment of any other agency employees with the title of CIO.<sup>5</sup>

In addition, in a variety of reports that we have issued since fiscal year 2010, we have made numerous recommendations aimed at improving federal IT management. Specifically, between fiscal years 2010 and 2015, we made 803 recommendations to OMB and federal agencies to address shortcomings in IT acquisitions and operations. As of January 2017, about 46 percent of these recommendations had been fully implemented. Further, to help address these ongoing challenges, we recently added improving the management of IT acquisitions and operations to our list of high-risk areas for the federal government.<sup>6</sup>

In fiscal year 2017, the government plans to invest more than \$89 billion for IT. Given the importance of the role that CIOs have in managing the government's portfolio and the challenges that federal agencies have encountered, this forum had a special focus on how CIOs can help improve IT delivery and operations.

To solicit ideas and suggestions on how to improve the government's delivery and operation of IT, thus creating a better functioning government, we convened and moderated a diverse panel of 13 current and former federal agency CIOs, members of Congress, and private sector IT executives. We selected these participants (listed in appendix I) to represent a range of viewpoints and backgrounds related to the acquisition and operation of federal IT. The forum agenda provided for structured discussions to allow each participant to comment openly and interact with other participants on any issue. This report summarizes the discussion by forum participants and highlights the ideas and themes that emerged from the forum.

The information and viewpoints summarized here do not necessarily represent the views of all participants or the views of their organizations or GAO. We did not independently assess the accuracy of the statements expressed by participants. We structured the forum so that participants could openly comment on the issues discussed, and not all participants commented on all the discussion topics. To ensure the accuracy of our summary, we provided participants the opportunity to review a summary

---

<sup>5</sup>40 U.S.C. § 11319(b)(1)(C)(i)(I), (b)(2).

<sup>6</sup>GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

of key points from the forum and incorporated their comments as appropriate prior to publishing this report.

We conducted our work from October 2016 to April 2017 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient, appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions in this product.

We plan to send copies of the report to appropriate congressional committees and interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>. Questions may be addressed to David A. Powner, Director, Information Technology Management Issues, at (202) 512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov). Contact points for our Office of Congressional Relations and Office of Public Affairs appear on the last page. Major GAO contributors are listed in appendix III.

We wish to thank all of the forum's participants for taking the time to share their knowledge and insights during the forum discussion. The breadth of observations and suggestions that were shared provided a solid foundation on which to build further improvement into how the federal government manages its significant investment in IT.



David A. Powner  
Director, Information Technology Management Issues

---

## Opportunities for Improving IT Acquisitions and Operations

This report summarizes key actions that emerged from the participants' discussion to improve federal IT acquisitions and operations. The key actions are organized under the following topics:

- strengthening the impact of FITARA,
- improving CIO authorities,
- budget formulation,
- governance,
- workforce,
- operations, and
- transition planning.

---

### Strengthening the Impact of FITARA

Recognizing the severity of issues related to the government-wide management of IT, FITARA was intended to improve agencies' acquisitions of IT and enable Congress to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings.

Forum participants agreed that FITARA is the government's best chance to improve federal agencies' IT acquisitions and operations. The participants viewed FITARA as having been partially effective to date, with positive developments having emerged since the law was passed. For example, they noted that the law has led to more collaboration among federal IT stakeholders and that congressional oversight facilitated by the FITARA scorecards<sup>7</sup> has highlighted the importance of, and visibility into, the implementation of the law.

Nevertheless, the participants emphasized that major barriers to full implementation of the law, such as organizational cultures, stand to limit

---

<sup>7</sup>The House Committee on Oversight and Government Reform monitors the implementation of FITARA by grading agencies' efforts using a scorecard.

its impact. Several participants noted the importance of Congress and the White House placing individuals knowledgeable in IT and cybersecurity issues as the heads of agencies. Otherwise, these participants believed FITARA could “go the way of Clinger-Cohen,”<sup>8</sup> a law that was well-intended, but which was not effectively implemented.

With these views in mind, the participants suggested three areas that could be addressed to help strengthen FITARA’s impact:

- Congressional oversight could be more aggressive,
- OMB may need to strengthen its role, and
- the Department of Defense should be required to implement all provisions of FITARA.

#### Congressional Oversight Could Be More Aggressive

The participants suggested that Congress could take several additional steps to enhance its oversight of the implementation of the reform legislation. Specifically, they said Congress could (1) impose more detailed implementation requirements if progress by the agencies does not continue, (2) enhance the scorecards by focusing on CIO authority, and (3) hold heads of agencies or deputy secretaries accountable by having them testify at FITARA oversight hearings. However, participants noted that Congress also could reduce oversight for agencies making good progress in their implementations.

#### OMB May Need to Strengthen Its Role

Participants commented that OMB did not support FITARA when the legislation was passed. Nevertheless, they noted that OMB’s guidance issued after the passage of FITARA has been quite positive in helping agencies implement the law’s requirements.

---

<sup>8</sup>The Clinger-Cohen Act of 1996 (Pub. L. No. 104-106, § 5125(c)(3) (Feb. 10, 1996), codified at 40 U.S.C. § 11315(c)(3)) placed responsibility for managing investments with the heads of agencies and established CIOs to advise and assist agency heads in carrying out this responsibility. Additionally, this law required OMB to establish processes to analyze, track, and evaluate the risks and results of major capital investments in information systems made by federal agencies and report to Congress on the net program performance benefits achieved as a result of these investments.

The participants believed that many of the agencies' FITARA implementation plans did not accurately reflect the true state of CIO authority challenges that existed at those agencies. However, the participants acknowledged that, to OMB's credit, many of the agencies' initial submissions of their plans were not approved by OMB and were sent back to agencies for revision. The participants stressed the importance of OMB having an active role following up on these plans to ensure that they are effectively implemented.

### The Department of Defense Should Be Required to Implement All Provisions of FITARA

Several forum participants noted that the largest agency in the federal government, the Department of Defense, does not have to comply with all provisions of FITARA.<sup>9</sup> However, participants stressed that the department should be required to implement all aspects of the law, given that it annually spends about one-third of the federal government's total IT dollars and has struggled with the management of its IT.

---

### Improving CIO Authorities

Federal law, particularly FITARA, has strengthened the role of the CIO as the focal point for IT management within agencies. Additionally, we have long been proponents of having strong agency CIOs in place to lead federal agencies in managing IT.

However, we have reported that CIOs have faced limitations in exercising their influence in certain IT management areas.<sup>10</sup> For example, not all CIOs had the authority to review and approve the entire agency IT portfolio; they do not always have sufficient oversight of IT investments; and they often had limited influence over the IT workforce, such as in hiring and firing decisions.

Further, forum participants noted that CIOs directly control and have visibility into a relatively small portion of the amounts available for IT

---

<sup>9</sup>The Department of Defense is excluded from requirements under certain provisions of FITARA, including those that require agency CIOs to (1) approve the IT budget requests of their respective agencies, (2) review and approve contracts for IT, and (3) approve the appointment of other agency employees with the title of CIO.

<sup>10</sup>[GAO-11-634](#).

spending. For example, a participant cited an example of one CIO who had budget authority over only \$80 million out of an overall \$2 billion IT budget.

The participants identified four actions that could help improve CIO authorities:

- have the CIO Council play an enhanced role in improving authorities,
- implement collaborative governance,
- evolve the role of the CIO to enable change, and
- focus on cybersecurity to change existing cultures.

#### Have the CIO Council Play an Enhanced Role in Improving Authorities

In addition to OMB, forum participants suggested that the CIO Council<sup>11</sup> play an enhanced role in improving authorities. Specifically, a participant stated that CIOs can act collectively through the Council to share best practices to the problems and challenges they confront. This sharing of successful practices can help CIOs make improvements at their respective agencies and strengthen their authorities. In addition, initiatives endorsed by the CIO Council with the backing of the Federal CIO<sup>12</sup> are often viewed as priorities and can help CIOs tackle key issues where historically their lack of authority was an issue. The participants agreed that, in the past, the CIO Council was quite active and effective sharing these best practices, though this is not the case today.

#### Implement Collaborative Governance

A participant suggested that agencies implement collaborative and interagency governance, as such an approach would bring together key agency executives to discuss investment performance, thus increasing accountability. Specifically, the participant said that a collaborative governance model strengthens executive relationships and is critical to

---

<sup>11</sup>The CIO Council is the principal interagency forum on federal agency practices for IT management.

<sup>12</sup>The Federal CIO is the administrator of the Office of E-Government and Information Technology within OMB, and oversees all federal IT spending, policy, and strategic planning.

exercising CIO authorities. The participant gave an example in which an agency with a mature governance approach and a collaborative relationship among agency executives (e.g., Chief Financial Officer and agency component leadership) had stopped 45 programs that were all a year behind schedule and 50 percent over budget, and had not delivered any functionality to users. The participant saw this as highlighting the importance of CIOs having positive relationships within the agency in order to have the authority and support to take such actions as stopping poorly performing projects.

#### Evolve the Role of the CIO to Enable Change

The participants felt the CIO role needs to evolve to where CIOs enable change more and that too often today the CIO role is focused heavily, if not entirely, on creating and enforcing policies and running IT operations. For example, a participant suggested that in addition to just enforcing policies, CIOs need to be trusted advisors to the agency head and strategic advisors, rather than just running IT operations. Further, the participant said that CIOs should enable change by focusing on how government can improve citizens' lives. In addition, a participant noted that this focus on just enforcing policies and running operations has contributed to CIOs missing out on opportunities to become forward-looking business drivers. The participant added that, as a result, many CIOs have been relegated to running infrastructure and are not viewed in their agencies as strategic enablers.

#### Focus on Cybersecurity to Change Existing Cultures

According to the participants, CIOs should have a keen focus on cybersecurity to help change cultures and improve authorities. Given the growing threats and severe consequences of cybersecurity incidents, the participants agreed that having cybersecurity as a priority could help to elevate the CIOs' role and their respective authorities. In this regard, a participant stressed the importance of agencies establishing strong cybersecurity policies that require CIO approval before systems become operational. Another participant stated that facilities, including laboratories and research facilities, should also have CIO oversight to ensure appropriate performance and cybersecurity.

---

---

## Budget Formulation

To help better understand the federal government's spending on IT, OMB requires agencies to identify all of their investments and the associated costs as part of their annual budget formulation processes.<sup>13</sup> OMB then uses this information to analyze, track, and evaluate the risks and results of all major IT investments.

However, our work has shown that agencies have been challenged in accurately capturing their IT budgets.<sup>14</sup> As a result, agencies submit budget information to OMB that is not always complete. This is due, in part, to the fact that CIOs do not always have control over the entire IT budget. In addition, the definition of IT can vary across agencies. We have reported that OMB's definition of an IT investment is broad, and agencies interpret it in different ways.

As a result, not all IT spending is included in the federal government's estimate. For example, our previous work found that the Department of Energy had reported several of its supercomputer investments, which accounted for \$368 million, as facilities rather than IT.<sup>15</sup> In addition, in that same report, we noted that the Department of Commerce did not report its satellite investments as IT, which accounted for \$447 million.

Recognizing these challenges, the forum participants identified five key actions that could be taken by federal agencies and OMB to help improve the formulation of IT budgets:

- use IT spend plans to improve budgets,
- examine agency programs to capture additional IT spending,
- simplify the definition of IT,
- work more closely with procurement organizations, and
- work with congressional committees to explore budgeting flexibilities.

---

<sup>13</sup>Office of Management and Budget, *Circular No. A-11* (Washington, D.C.: July 1, 2016).

<sup>14</sup>GAO, *Information Technology: OMB Needs to Improve Its Guidance on IT Investments*, [GAO-11-826](#) (Washington, D.C.: Sept. 29, 2011).

<sup>15</sup>GAO, *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available*, [GAO-14-64](#) (Washington, D.C.: Dec. 12, 2013).

---

### Use IT Spend Plans to Improve Budgets

The forum participants suggested that agencies could strengthen the formulation of their IT budget requests by making greater use of IT spend plans<sup>16</sup> to identify their costs more completely. For example, one of the participants noted an agency, consisting of multiple bureaus, that relies on a two-pronged approach to using spend plans to help capture IT costs: the agency's FITARA action officer ensures that each bureau CIO submits an IT spend plan to the agency's budget office, and major program managers are also required to share these spend plans with the budget office. By doing so, the agency has been able to achieve positive collaboration between the bureaus and program managers, and consequently, has increased visibility into the identification and reporting of its IT spending.

Additionally, in noting the benefits of spend plans, one of the participants pointed to an agency that had used these plans to identify and consolidate 50 duplicative local area networks—an action that saved millions of dollars. Another participant reported that one agency had captured detailed spend plans across all of its components by involving both program offices and the field in the budgeting process, which provided a better understanding of how the field was using IT.

The participants stressed the importance of having top-level executive support to ensure that spend plans are appropriately used throughout the agency. They noted that such support is critical to more completely capturing an agency's spending. One participant suggested that CIOs forming partnerships with component agencies as part of the budgeting process is vital to ensuring executive support for spend plans. Another participant stated that management authority should not be underestimated and that if the agency head insists on using spend plans, then there is a greater chance that they will be used.

On the other hand, a participant cautioned that while OMB has in the past tried to link an IT spend plan approach to the President's budget submission, the results have not always ensured a full accounting for IT spending. Moreover, participants noted that OMB's tools for capturing IT

---

<sup>16</sup>A spend plan documents all planned IT within each annual appropriation, and ties investments to contracts, which improves the tracking of IT obligations and expenditures.

---

spending, the exhibit 300 and the exhibit 53,<sup>17</sup> are not always accurate and that they are viewed far too often as a compliance exercise.

### Examine Agency Programs to Capture Additional IT Spending

The participants proposed addressing the challenge of capturing all IT spending by focusing more attention on an agency's programs, since all programs have an IT component. In their view, an agency would be better positioned to capture more detailed information on IT spending by examining the IT embedded within its programs and ensuring that the programs are being managed with the right IT-related people and governance processes. These participants added that such an approach could address the fact that it can be difficult to identify the IT components of overall programs.

Further, participants stated that taking such a program-centric approach is important since precisely capturing all IT spending within a larger program is difficult. Additionally, a participant suggested that focusing on programs to identify IT spending was more strategic, and could enable the CIO to function more like a strategic-focused private sector CIO instead of just being responsible for the numerous requirements imposed on federal CIOs by law and federal policies.

### Simplify the Definition of IT

Forum participants commented that the President's budget submission may not capture all of the government's IT spending due to the varying interpretations of the current definition of IT. A participant noted that simplifying the definition may help address this challenge.

One participant offered that providing a simpler definition of IT would make it more difficult for agencies to take liberties with the definition, and thus, exclude programs that are clearly IT. As an example, the participant cited programs such as the Department of Defense's reconnaissance satellites and some of the Department of Commerce's and the National Aeronautics and Space Administration's investments that are not classified as IT, even though these programs have large IT components.

---

<sup>17</sup>OMB uses several data collection mechanisms during the annual budget formulation process to oversee federal IT. Specifically, OMB requires federal departments and agencies to provide information related to their business cases through the exhibit 300 and IT portfolio report, known as the exhibit 53.

Another participant suggested that a possible approach could be to define IT as anything that can be “networked or hacked.” The participant stated that doing so would help improve how IT spending is captured, as such a definition would encompass anything attached to an information network, or that could be electronically compromised.

In addition to simplifying the definition, a participant stated that OMB could take a greater role in identifying IT that is not reported in the budget. The participant felt that OMB could help to resolve this problem of unidentified IT by not permitting agencies to exclude such expenditures from their IT budget requests.

#### Work More Closely with Procurement Organizations

Forum participants discussed the value in working more closely with agency procurement organizations as another means of ensuring that IT spending will be captured. According to the participants, an agency CIO could benefit from working closely with the agency’s procurement office and procurement process to identify IT-related contracts and their associated costs. One example was provided where an agency CIO decided to look at credit card purchases, which provided a more granular level of funding information than had been previously available.

In addition, one of the participants noted an example of an agency CIO that had statutory authority over the department’s IT budget and, as a result, had created a centralized budget process. This process required every proposed departmental acquisition possibly involving IT to be identified by the agency’s procurement office and sent to the CIO, who then determined if the acquisition was to be included in the budget. These approved acquisitions were then included in an annual operating plan for IT that was developed each year.

#### Work with Congressional Committees to Explore Budgeting Flexibilities

The participants talked about the importance of CIOs working with congressional committees, especially the appropriations committees, specifically to allow for budgeting flexibilities. They pointed out that agency budget requests are to be submitted to OMB far in advance of the

---

beginning of each fiscal year.<sup>18</sup> As a result, the budget may not be reflective of exact IT needs once the budget is released and agencies might need to explore opportunities to make adjustments.

One participant specifically cited the example of an agency whose CIO was allowed the flexibility by Congress to reprogram previously appropriated funds within the first 30 days of the fiscal year, and thus was able to adjust year-old budget proposals to meet current needs. The participant felt that such flexibility should be considered for other federal agencies, as it was a private sector best practice. Another participant noted that an additional flexibility that would be helpful would be allowing agencies to roll over unused obligational authority into the next year, so that funds could continue to be spent on agency priorities, which agencies are currently not allowed to do.

---

## Governance

Effective IT governance depends on agencies having sound investment management processes that position them to attain successful, predictable, and repeatable investment control and oversight. Such oversight should be the responsibility of agency CIOs and other executives, including Chief Financial Officers and executives of major bureaus and component agencies for whom the technology is serving, to ensure that technical, financial, and business needs are all addressed.

However, we have previously reported that executive-level governance and oversight of federal IT has often been ineffective. For example, we have reported on governance boards that either have not held oversight meetings<sup>19</sup> or have not sufficiently addressed risks as part of this process.<sup>20</sup> As a result, we noted numerous federal IT projects that have failed due to a lack of effective governance, oftentimes resulting in millions of dollars wasted.

---

<sup>18</sup>According to OMB's Circular A-11, which provides annual guidance on preparing, submitting, and executing the federal budget, agencies are required to submit their budget proposals to OMB more than a year in advance. For example, proposed budgets for fiscal year 2017, which began in October 2016, were due in September 2015.

<sup>19</sup>GAO, *Healthcare.gov: Ineffective Planning and Oversight Practices Underscore the Need for Improved Contract Management*, GAO-14-694 (Washington, D.C.: July 30, 2014).

<sup>20</sup>GAO, *IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments*, GAO-16-494 (Washington, D.C.: June 2, 2016).

Six suggested actions emerged from the forum discussions that could help address governance challenges:

- obtain support from agency leadership,
- enhance governance at OMB and agencies,
- use security authorities to enhance governance,
- strengthen oversight for IT purchased as a service,
- buy more and develop less, and
- evolve procurement processes to align with new technologies.

#### Obtain Support from Agency Leadership

The participants stressed that agency leadership (e.g., secretaries and deputy secretaries) is key to effectively implementing an IT governance process. Agency leadership needs to clearly understand the role of IT and to set the expectation regarding the importance of executive-level governance. Some of the participants noted that the head of the agency is best positioned to help change the organizational culture by setting the tone at the top and providing support for CIOs. This support is also essential to ensure that CIOs have adequate authority to effectively govern.

#### Enhance Governance at OMB and Agencies

The forum participants pointed to the importance of the OMB and specifically, the role of the Federal CIO, to help ensure effective IT governance. They saw this role as continuing to grow in importance, noting for example, that the Federal CIO has provided important leadership on cybersecurity, acquisition, and operations initiatives. The participants cited specific OMB initiatives undertaken by the Federal CIO, like the cybersecurity sprint,<sup>21</sup> TechStats sessions, and data center consolidation efforts that resulted in greater accountability and positive results. For example, TechStat sessions were led by the Federal CIO,

---

<sup>21</sup>Following a cybersecurity breach at the Office of Personnel Management in 2015, OMB initiated a cybersecurity sprint. This initiative identified a set of critical cybersecurity actions for federal agencies to take within 30 days and established a sprint team to review the federal government's cybersecurity policies. The sprint team's recommendations led to an October 2015 OMB memorandum titled "Cybersecurity Strategy and Implementation Plan."

involved agency leadership, and addressed troubled IT projects. These sessions resulted in projects being more effectively managed, as well as several terminations for those projects that were failing.

As an additional example, a participant noted that a former OMB executive held meetings with agency secretaries during Y2K which, in turn, had sent a message that Y2K was not only a CIO problem, but also an agency-wide issue.<sup>22</sup> OMB's leadership led to an effective federal approach to the Y2K challenge according to our participants. A participant added that, in order to bring about change at the cabinet level and among leadership across all agencies, OMB must play a critical role.

The participants also stressed that the agencies themselves can play a more significant role in enhancing IT governance. One participant stated that agency governance can result in better management and delivery of IT. Another participant noted that active governance boards that discuss program performance, risks, and solutions on major IT acquisitions helps to ensure a clear direction on projects.

Participants also said that measuring the maturity of agencies' IT management could enhance governance. They referred to existing process maturity models that could be used, including a recent American Council for Technology and the Industry Advisory Council model.<sup>23</sup> Further, the participants stated that in addition to measuring outputs and results, there is also value in measuring process maturation over time since it has been proven that mature processes help with delivering IT results. They suggested that we have a continued role in measuring process maturity with our audits.

### Use Security Authorities to Enhance Governance

Forum participants acknowledged that it can be difficult for a governance approach to be effective if a CIO does not have the appropriate authorities to carry out the governance responsibilities. As such, they suggested that an alternative way to assert authority could be to leverage security responsibilities. One participant cited an example where a CIO

---

<sup>22</sup>Y2K, also called the year 2000 bug or millennium bug, was a problem in the coding of computerized systems that was projected to create havoc in computers and computer networks around the world at the beginning of the year 2000.

<sup>23</sup>This council is a non-profit educational organization established to improve government through the effective and innovative application of technology.

was frustrated with the agency's ineffective IT governance at the agency and decided to conduct a comprehensive security exercise to highlight why such governance was needed. Specifically, this participant contracted with an engineering firm to obtain an overall inventory of every device and system on the agency's physical network. The CIO then compared this inventory to the IT inventories received from the agency components and discovered many instances of IT that the agency components were unaware of. In addition, the participant noted that, in this example, many of the unknown devices and systems were not properly secured (i.e., not patched correctly, with factory default usernames and passwords). This effort garnered the attention of the agency secretary, which resulted in the agency components working more closely with the CIO. The participant stated that the strategy of using security responsibilities helped to highlight the critical governance role a CIO should perform.

### Strengthen Oversight for IT Purchased As a Service

The forum discussion addressed the fact that the federal government purchases a large portion of its IT as a service and that this is expected to increase with the move toward more cloud computing<sup>24</sup> and shared services.<sup>25</sup> As such, the participants saw the need for oversight of this area to be strengthened. In this regard, a participant stated that IT as a service is not included to the extent needed in agencies' governance processes. The participants added that IT as a service should be included in agencies' governance processes to ensure that there are appropriate contracts in place and that appropriate oversight of performance occurs. They further suggested that contractual service-level agreements be the focus of this oversight in order to ensure that purchased services are meeting performance, security, and other agency requirements.

### Buy More and Develop Less

The participants suggested that agencies consider buying more commercial IT products that can be used as delivered and developing fewer IT systems. In their view, doing so would result in more effective

---

<sup>24</sup>Cloud computing is a means for enabling on-demand access to shared and scalable pools of computing resources with the goal of minimizing management effort or service provider interaction.

<sup>25</sup>IT functions that are provided for consumption by multiple organizations within or between federal agencies are known as shared services.

---

delivery of IT. However, the participants acknowledged that this approach would require, in most instances, modifying existing business processes to accommodate the purchased systems. They added that the government's general reluctance to change business processes is a major reason why, historically, the federal government has not purchased commercial IT products to the extent that it should.

Nevertheless, one participant provided an example of an organization that successfully did so: Apple Inc. implemented financial control and reporting software without any modifications to the commercial product and subsequently, changed its business processes to work with this new software. In line with this example, one participant stressed that agencies should consider buying more commercial products and modifying them as little as possible. The participants considered this approach to be especially applicable to financial management systems, since many of these acquisitions have failed due to excessive modifications—resulting in billions wasted.

### Evolve Procurement Processes to Align with New Technologies

The participants discussed the importance of federal agencies' IT procurement offices and processes evolving with the newer technologies. In their view, the government procurement processes can be "too traditional." The participants added that agencies are not always set up to take advantage of more modern offerings, such as cloud services and acquisitions using agile development processes.<sup>26</sup> One participant noted that, in her experience, the government may not explore all procurement opportunities that are available to it. As a result, there is less ability to tap innovation.

---

## Workforce

The federal government has been challenged in its efforts to attract qualified CIOs and a robust IT workforce. Challenges in attracting qualified CIOs are due to several factors, including, according to our participants, the lower pay in government as compared to the private sector and the limited authorities given to federal CIOs. As a result, the

---

<sup>26</sup>Agile development is an incremental approach that delivers software functionality in short increments before the system is fully deployed.

federal government does not consistently attract strong and accountable CIOs to manage federal IT acquisitions and operations.

Additionally, federal agencies have not demonstrated effective IT workforce planning. This is important to an agency's success in developing the necessary knowledge, skills, and abilities to execute a range of management functions that support the agency's mission and goals. Federal law and guidance over the past 20 years has called for agency CIOs to assess agency personnel regarding their IT knowledge and skill requirements, identify gaps in meeting those requirements, and develop strategies and plans to address deficiencies. Nevertheless, over the past several years, we have repeatedly reported that agencies across the federal government have not always effectively planned for IT workforce challenges.<sup>27</sup>

The forum participants suggested five actions related to addressing the government's challenges with acquiring an IT workforce:

- attract more qualified CIOs by appealing to key missions,
- have the Federal CIO play a more active role in attracting agency CIOs,
- give CIOs more human resource flexibilities,
- focus on attracting and investing in a more holistic IT workforce, and
- better integrate private sector talent into the IT workforce.

#### Attract More Qualified CIOs by Appealing to Key Agency Missions

Forum participants stated that the importance of agencies' missions, such as securing the homeland and better serving our veterans, needs to be a major factor in attracting more qualified CIOs to the federal government. Several participants stated that this is what attracted them to federal CIO

---

<sup>27</sup> See, for example, GAO, *2020 Census: Key Challenges Need to Be Addressed to Successfully Enable Internet Response*, [GAO-15-225](#) (Washington, D.C.: Feb. 5, 2015); *Federal Emergency Management Agency: Additional Planning and Data Collection Could Help Improve Workforce Management Efforts*, [GAO-15-437](#) (Washington, D.C.: July 9, 2015); *2020 Census: Key Information Technology Decisions Must Be Made Soon*, [GAO-16-205T](#) (Washington, D.C.: Nov. 3, 2015); *Information Technology: FEMA Needs to Address Management Weaknesses to Improve Its Systems*, [GAO-16-306](#) (Washington, D.C.: Apr. 5, 2016); and *VA IT Management: Organization Is Largely Centralized; Additional Actions Could Improve Human Capital Practices and Systems Development Processes*, [GAO-16-403](#) (Washington, D.C.: Aug. 17, 2016).

jobs. The participants added that having both government and private sector experience is valuable for CIOs, and they stressed that more effort needs to be given to recruiting private sector CIOs at “the right time in their careers” because many are interested in working for the federal government. Further, a participant suggested that 5-year term appointments for CIO positions should be considered in order to transcend administrations. The participant added that term appointments could be viewed as more attractive to many potential CIOs since such appointments would allow more time to influence change within the agencies.

#### Have the Federal CIO Play a More Active Role in Attracting Agency CIOs

The participants believed the Federal CIO should play a role in attracting agency CIOs. They viewed the Federal CIO as being in a unique position with White House backing to help recruit CIOs to the federal government. One suggestion offered by the participants was that the Federal CIO create a pool of highly skilled CIOs by establishing three to five CIO advisory positions working with the Federal CIO at OMB. These advisors would work initially at OMB and then be available when an agency CIO position is vacant. The participants felt that such a strategy would be beneficial because these CIOs would already be known and trusted in OMB. As an example, one participant cited a former Deputy Federal CIO at OMB executive who had recently become the CIO at the Office of Personnel Management, thereby allowing someone with direct OMB experience to move into an agency role.

#### Give CIOs More Human Resource Flexibilities

A key concern was raised by participants regarding the way in which the federal government develops its IT workforce. In particular, they stated that CIOs can inherit IT staff, some of whom are not the most qualified. With this in mind, the participants stated that CIOs should be given more human resource flexibilities so that they can attract, retain, and manage talent appropriately. The participants noted that CIOs should be able to build their own teams and hold them accountable; they added that CIOs

---

should be empowered to tell employees when their services are no longer required. One specific suggestion was to give CIOs direct hire authority.<sup>28</sup>

### Focus on Attracting and Investing in a More Holistic IT Workforce

Forum participants suggested that agencies could benefit from attracting and investing in a more holistic IT workforce—that is a workforce that includes the right disciplines and effectively integrates contractors. A participant noted that the government IT workforce needs to be viewed and managed in a blended way that includes contractors and other industry professionals.

One participant observed that the government has struggled to hire key technologists, such as cyber experts, network engineers, and software developers. The participant suggested that the government needs to work with colleges and universities to attract these disciplines. Overall, the participants agreed that this issue, especially for cyber, is not just a government issue, but also a national and global issue. For example, one participant spoke of a private sector company that had lost key cybersecurity employees to companies in other countries that paid them three times their private sector salaries.

### Better Integrate Private Sector Talent into the IT Workforce

The participants discussed the need for better integration between the private sector and the federal IT workforce. Specifically, they stated that the U.S. Digital Service and 18F teams are not well integrated with federal IT/CIO organizations, which had created a “we versus them” environment.<sup>29</sup> The participants noted the highly qualified staff at U.S. Digital Service and 18F and stated that these centralized pools of private sector talent need to be better integrated with the federal IT workforce. Participants also noted the need for better integration in “blended workforces,” where industry and government work together.

---

<sup>28</sup>Human resource flexibilities may exempt agencies from civil service requirements under federal law.

<sup>29</sup>In an effort to improve federal IT management, in March 2014 the General Services Administration established 18F, a team of expert designers, developers, technologists, researchers, and product specialists, that provide IT services (e.g., develop websites and provide software development training) to federal agencies on a reimbursable basis. In addition, in August 2014, OMB established U.S. Digital Service, a team of private sector experts and leading civil servants, aims to improve public-facing federal IT services.

---

---

## Operations

With much of the amount reportedly spent on operating and maintaining existing (legacy) IT systems, it is important that agencies effectively manage their operations and maintenance (O&M). In this regard, we recently reported that in fiscal year 2015, of the more than \$80 billion reportedly spent on federal IT, the federal government spent about 75 percent on O&M investments.<sup>30</sup> Such spending had increased over the past 7 fiscal years, and alternatively, resulted in a \$7.3 billion decline from fiscal years 2010 to 2017 in IT development, modernization, and enhancement activities.

Further, federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported, creating significant security risks. OMB recently began an initiative to modernize, retire, and replace the federal government's legacy IT systems; however, until agencies fully execute this initiative, the government runs the risk of maintaining systems that have outlived their effectiveness.

In addition, we have issued a series of reports regarding data center consolidation.<sup>31</sup> We have pointed out that, while consolidating data centers has resulted in almost \$3 billion in savings, weaknesses existed in the execution and oversight of this initiative.<sup>32</sup> In particular, planned savings may have been understated because of difficulties agencies had encountered when calculating savings and communicating their estimates to OMB.

---

<sup>30</sup>GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, [GAO-16-468](#) (Washington, D.C.: May 25, 2016).

<sup>31</sup>OMB launched the Federal Data Center Consolidation Initiative in 2010, which was then superseded in 2016 by the Data Center Optimization Initiative.

<sup>32</sup>GAO, *Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established [Reissued on March 4, 2016]*, [GAO-16-323](#) (Washington, D.C.: Mar. 3, 2016); *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings*, [GAO-14-713](#) (Washington, D.C.: Sept. 25, 2014); *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal*, [GAO-13-378](#) (Washington, D.C.: Apr. 23, 2013); *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed*, [GAO-12-742](#) (Washington, D.C.: July 19, 2012); and *Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings*, [GAO-11-565](#) (Washington, D.C.: July 19, 2011).

As such, to address these challenges with operations, the participants suggested that agencies and CIOs could take the following three actions:

- use a strategic approach for legacy system migration,
- migrate more services to the cloud, and
- implement strategies to mitigate the impact on jobs when closing data centers.

### Use a Strategic Approach for Legacy System Migration

The participants suggested that agencies and CIOs take a strategic approach to legacy migration to replace outdated systems that focuses more on addressing security vulnerabilities and mission performance than only on the fact that systems are outdated. One participant stated that the argument that “legacy systems still work” is not valid because many of these older systems are expensive to maintain and mission performance has not improved for decades in some instances. Another participant stated that agencies could use a multiyear system disposition strategy to establish firm deadlines to decommission legacy systems. Further, according to the participants, legacy migration needs to include in the strategic approach a focus on changing business processes. One participant noted that many of the problems with legacy systems are really issues with inefficient legacy business process issues.

### Migrate More Services to the Cloud

Participants also pointed out that agencies need to migrate more data and services to cloud computing. In their view, this approach would offer agencies a means to buy the services faster and possibly cheaper than through the traditional methods of building and maintaining systems. A participant cited one department’s move from data centers to the cloud, noting that doing so had allowed the department to get out of the infrastructure business and reduce its number of data centers. Another participant cited a department that worked with its Chief Financial Officer to acquire cloud services that resulted in a bureau where almost everything has fully migrated to the cloud. Our participants stressed that too many agencies use security as an excuse for not wanting to move to cloud services, when in fact, organizations that require high security, like the Central Intelligence Agency, are already making the transition.

---

### Implement Strategies to Mitigate the Impact on Jobs When Closing Data Centers

Forum participants cautioned that the ongoing government-wide data center consolidation effort could face employee resistance due to the potential loss of jobs that results from some data center closures. One strategy that was suggested was to reduce the functions and the associated positions of those data centers gradually over time to lessen the chances of resistance. Eventually the centers would be performing limited functions and have limited full-time employees associated with them. Thus, phasing them out could become a less sensitive issue.

---

### Transition Planning

Effective presidential administration transition planning is extremely important as it relates to IT. Specifically, such planning should focus both on making improvements to the prior administration's efforts but also on ensuring that progress agencies have made is not lost going forward. This is especially key for ensuring that both the challenges and the momentum with implementing FITARA is acknowledged.

Participants suggested four actions to ensure there is a focus on IT when an administration transition occurs, including the appointment of new agency CIOs:

- convey IT and cyber issues early to leadership,
- encourage Congress to focus on IT and cybersecurity at confirmation hearings,
- ensure that IT and cyber issues are OMB priorities, and
- ensure GAO plays a role highlighting its work and expertise.

### Convey IT and Cyber Issues Early to Leadership

Forum participants re-emphasized the importance of conveying IT and cyber issues early in the transition phase to agency leadership. The participants stated that both FITARA and the focus on cybersecurity has resulted in more attention to these matters, but that if these topics are not stressed early during a transition, this attention and related progress could be lost. Further, one participant noted that previous administrations historically have focused attention in critical areas early on, so it is

important that major cyber and IT issues are an early focus with agency leadership.

### Encourage Congress to Focus on IT and Cybersecurity at Confirmation Hearings

A participant observed that even greater Congressional leadership regarding IT and cybersecurity issues is needed during a presidential transition. The participant further noted that, historically, Congress has asked some questions regarding IT and cybersecurity at confirmation hearings. It was suggested that this practice continue to make it very clear to incoming cabinet secretaries that these topics are Congressional priorities.

### Ensure That IT and Cyber Issues Are OMB Priorities

In addition to Congress, participants stated that OMB is key to ensuring that IT and cyber issues are priorities early in an administration, and one participant added that OMB is critical to clearly communicating the importance of these issues. Further, a participant observed that OMB plays an important role in overseeing the implementation of FITARA and providing guidance, such as its “common baseline” guidance, to improve CIO authorities.<sup>33</sup> The participant stressed the need for continued implementation of this guidance.

### Ensure GAO Plays a Role Highlighting Its Work and Expertise

GAO is cited in the Presidential Transition Act of 1963 as an agency that provides advice during the transition from one administration to the next.<sup>34</sup> GAO has several other resources at hand, such as priority recommendation letters to heads of agencies (which specifically address high-risk areas on information security and IT acquisition and operations),

---

<sup>33</sup>In June 2015, OMB released guidance that reinforces the importance of agency CIOs and describes how agencies are to implement FITARA. Among other things, this guidance outlined a “common baseline” of roles and responsibilities of agency CIOs and other senior agency officials related to 17 topic areas (common baseline sections), such as planning program management, reviewing and approving the IT budget request, and developing the IT workforce.

<sup>34</sup>See 3 U.S.C. § 102 note – Sec. 3(a)(8)(A)(ii)(III).

---

a high-risk report,<sup>35</sup> and a transition-related mobile application that all agencies can access.

Participants agreed that GAO has an important role to play in a presidential transition. Specifically, participants noted that GAO played a critical role in a previous administration transition by highlighting its work and expertise in meetings with the new Federal CIO and agency CIOs. Additionally, a participant said that GAO should not just rely on CIOs to read its full reports, and emphasized the importance of meeting and briefing a new administration.

---

<sup>35</sup>Every 2 years at the start of a new Congress, GAO calls attention to agencies and program areas that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation.

## Appendix I: Participants in the September 2016 Comptroller General Forum on IT Acquisitions and Operations

**Jonathan Alboum**

Chief Information Officer, U.S. Department of Agriculture

**The Honorable Roger Baker**

Consultant, Roger Baker Consulting, LLC

*Former Chief Information Officer, U.S. Department of Veterans Affairs*

**Dan Chenok**

Executive Director, IBM Center for the Business of Government

*Former Chief, Information Technology Branch, Office of Management and Budget*

**Casey Coleman**

Group Vice President, Civilian Agencies, Unisys Corporation

*Former Chief Information Officer, General Services Administration*

**The Honorable Gerald E. Connolly**

House of Representatives, Virginia, 11<sup>th</sup> District

Ranking Member, Subcommittee on Government Operations, Committee  
on Oversight and Government Reform

**Steve Cooper**

Chief Information Officer, U.S. Department of Commerce

**The Honorable Tom Davis**

Director of Federal Government Affairs for Deloitte, LLP

*Former Member of the House of Representatives, Virginia, 11<sup>th</sup> District*

*Former Chair, Committee on Oversight and Government Reform*

**Karen Evans**

National Director, U.S. Cyber Challenge

*Former Administrator of the Office of Electronic Government and  
Information Technology, Office of Management and Budget*

**The Honorable Will Hurd**

House of Representatives, Texas, 23<sup>rd</sup> District  
Chair, Subcommittee on Information Technology, Committee on  
Oversight and Government Reform

**Vivek Kundra**

Executive Vice President, Salesforce  
*Former Federal Chief Information Officer*

**Dave McClure**

Chief Strategist, Veris Group, LLC  
*Former Associate Administrator, Office of Citizen Services and Innovative  
Technologies, General Services Administration*

**Richard McKinney**

Chief Information Officer, U.S. Department of Transportation

**Richard Spires**

Chief Executive Officer, Learning Tree International  
*Former Chief Information Officer, U.S. Department of Homeland Security  
Former Chief Information Officer, Internal Revenue Service*

# Appendix II: Forum Agenda

<b>COMPTROLLER GENERAL FORUM</b> on IT Acquisitions and Operations	
<b>Opening Remarks</b> ..... 8:30-8:45a Rep. Gerry Connolly	<b>WEDNESDAY</b> <b>September 14, 2016</b>
<b>Opening Remarks</b> ..... 8:45-9a Gene Dodaro, Comptroller General	
<b>Budget Formulation</b> ..... 9-9:50a	<b>Sub-topics</b> <ul style="list-style-type: none"> <li>• Programming and budgeting decisions on IT</li> <li>• Capturing IT costs / “Shadow” (hidden) IT</li> <li>• IT acquisition contract approval</li> <li>• IT maintenance spend</li> <li>• Spending on mission critical vs. non-major systems (e.g., commodity IT)</li> <li>• Legacy IT funding strategies</li> <li>• Long-term, capital improvement (e.g., infrastructure) acquisition strategies</li> <li>• Attention to cybersecurity</li> <li>• Relationships and support with other senior managers</li> </ul>
<b>Governance and Oversight</b> ..... 10-10:50a	<ul style="list-style-type: none"> <li>• CIO visibility—troubled acquisitions, non-major acquisitions, O&amp;M investments</li> <li>• Conflicts with component IT and business managers</li> <li>• CIO reporting chain</li> <li>• CIO representation on non-IT boards</li> <li>• Tiered governance structures</li> <li>• Delegation of oversight responsibilities for acquisitions</li> <li>• Incremental development and delivery of IT acquisitions</li> <li>• Attention to cybersecurity</li> <li>• Relationships and support with other senior managers</li> </ul>
<b>Operations</b> ..... 11-11:50a	<ul style="list-style-type: none"> <li>• Types of barriers: political, cultural, mission-related</li> <li>• Data centers</li> <li>• Cloud</li> <li>• Legacy system modernization/transition</li> <li>• IT hardware and software inventory (including licenses)</li> <li>• Attention to cybersecurity</li> <li>• Relationships and support with other senior managers</li> </ul>
<b>Forum Luncheon</b> ..... 12-1p Guest—Rep. Will Hurd	
<b>Workforce</b> ..... 1-1:50p	<ul style="list-style-type: none"> <li>• Attracting top talent, including CIOs</li> <li>• Addressing skill gaps</li> <li>• Attention to cybersecurity</li> <li>• Relationships and support with other senior managers</li> </ul>
<b>Transition Planning</b> ..... 2-2:50p Guest—Tom Davis will address Congressional oversight and transition planning issues	<ul style="list-style-type: none"> <li>• Transitioning to a new Congress</li> <li>• Transitioning to a new Administration</li> <li>• Importance of a CIO Council</li> <li>• Level of focus from Congress in overseeing IT</li> <li>• CIO term appointments</li> <li>• Attention to cybersecurity</li> <li>• Relationships and support with other senior managers</li> </ul>
<b>Improving CIO Authorities</b> ..... 3-3:50p	<ul style="list-style-type: none"> <li>• FITARA implementation plans</li> <li>• Federal CIO</li> <li>• Attention to cybersecurity</li> </ul>
<b>Wrap Up</b> ..... 4-4:30p	

---

## Appendix III: GAO Contact and Staff Acknowledgments

---

### GAO Contact

David A. Powner, Director, Information Technology Management Issues;  
202-512-9286 or [pownerd@gao.gov](mailto:pownerd@gao.gov)

---

### Staff Acknowledgments

In addition to the contact named above, the following staff made key contributions to this report: Dave Hinchman, Assistant Director; Scott Borre; Rebecca Eyler; Josh Leiling; and Tina Torabi, Analyst-in-Charge.

---

---

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

---

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

Contact:

---

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

---

## Congressional Relations

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

---

## Public Affairs

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

---

## Strategic Planning and External Liaison

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