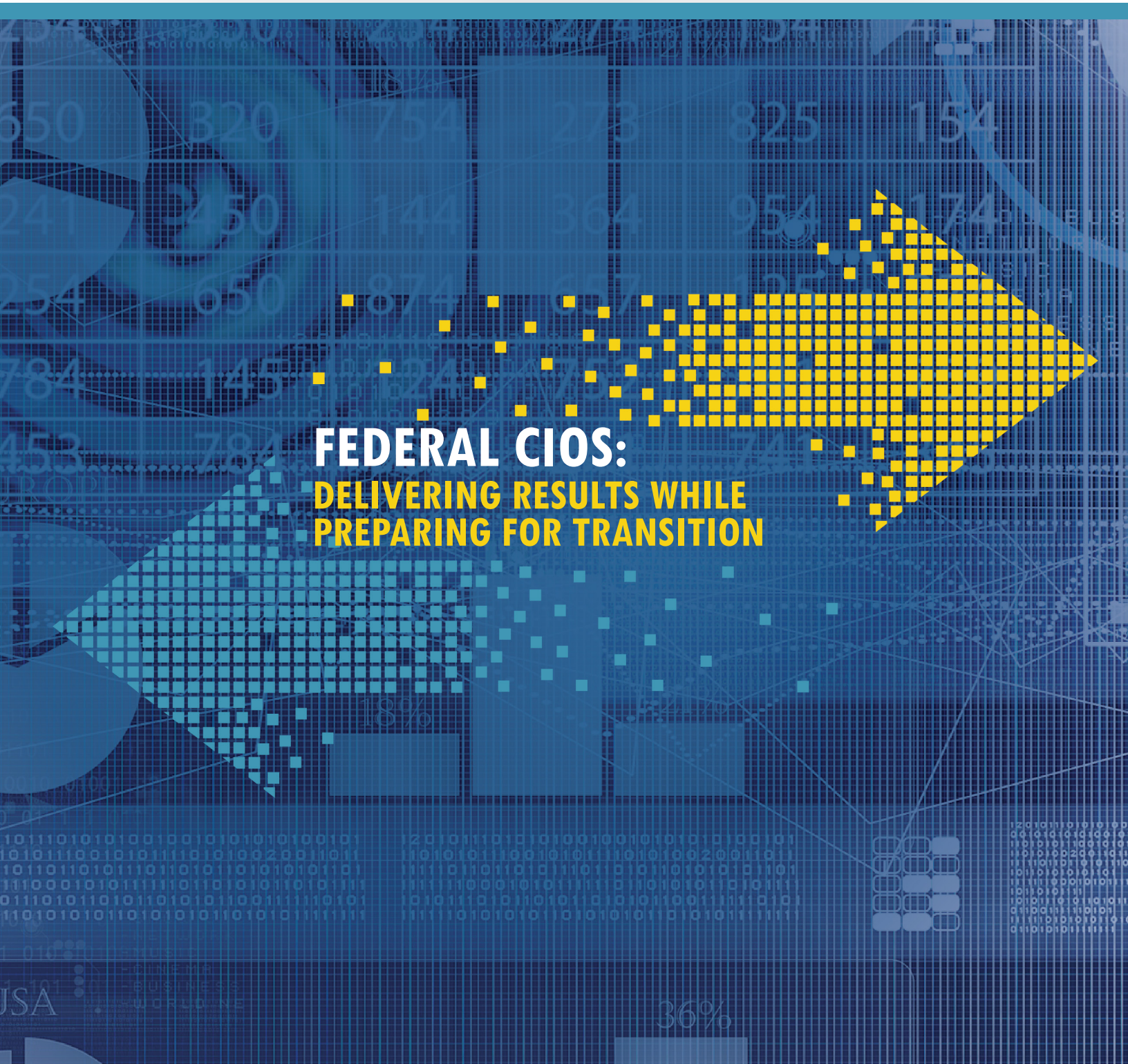
Grant Thornton

PSC PROFESSIONAL SERVICES COUNCIL

THE 2016 FEDERAL CIO SURVEY

SEPTEMBER 2016

26TH ANNIVERSARY



FEDERAL CIOS:

DELIVERING RESULTS WHILE PREPARING FOR TRANSITION

TABLE OF CONTENTS

ABOUT THE SURVEY

This survey is sponsored and led by the Professional Services Council (PSC) and PSC member company Grant Thornton. Grant Thornton has surveyed federal CIOs for 26 years. In recent years, the survey has expanded to include CISOs as well. Through these surveys, top IT officials, oversight groups, and congressional staff shared their views on challenges facing federal CIOs and the federal IT community. As in past years, PSC and Grant Thornton have received outstanding support from the federal CIO/CISO community in conducting this survey.

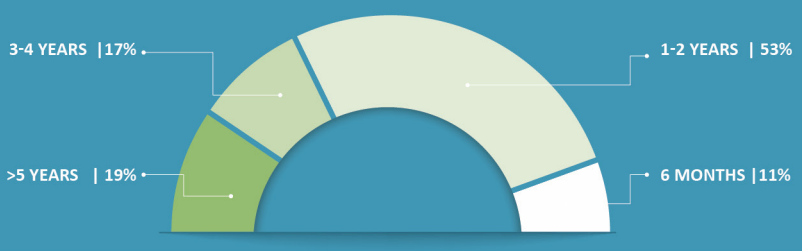
To preserve anonymity, we do not attribute responses to specific individuals. Readers may download copies of this and prior surveys at www.pscouncil.org

CONDUCTED INTERVIEWS

May 2016 to September 2016

INTERVIEWED 41 CIOs, CISOs, and Information technology officials

INSIGHTS FROM 23 AGENCIES



EXECUTIVE SUMMARY

2016 marks the 26th annual survey of CIOs, CISOs, and other key IT executives in the federal government and the pace of change those leaders have been experiencing continues to accelerate. Agency IT leaders are being asked to do more, do it better, and do it with less money. They are continuing to strive to balance oversight of operations for mission critical functions, opportunities to bring innovative services and efficiencies into government and building more effective cyber defenses as the threats to government systems continue to increase, often without access to financial investments to meet all these demands.

Even though the Obama administration is in its final year, the focus on government continuing to innovate and improve the quality and efficiency of government services and products through better technology has never been greater. One of the main drivers of this focus was the administration's budget proposal to create a $3.1 Billion IT modernization fund, which has sparked great discussions and debate from one end of Pennsylvania Avenue to the other about the best way to help government transition legacy systems heavy on operating costs to a more lean and agile government IT infrastructure.

In addition to a strong focus on the need for IT modernization and improved cybersecurity, the administration has not slowed down on launching new tools and initiatives designed to help agencies achieve that transition to modern digital services.

In just the last six months, the administration has launched a number of initiatives, including Category Management (improving the efficiency of purchasing laptops/desktops, software, and mobile devices), a new framework and playbook for modernizing mission support functions, the first ever Cybersecurity Workforce Strategy, updated guidance on data center consolidation, and a long-awaited update to OMB Circular A-130 – a foundational document to the way agencies manage information technology, security, data, and privacy across the government. CIOs and CISOs are right in the middle.

As expected, this year's survey respondents had wide-ranging views of these many initiatives, and working to integrate those new requirements into an already packed agenda has proved challenging. Although there are a host of new initiatives that are continuing to drive the IT agenda in agencies, CIOs and CISOs interviewed for this survey continue to cite similar challenges as in previous years. The main challenges and themes these executives struggle with include using an antiquated and bloated acquisition process, preparing adequately to protect federal networks and data amid rapidly increasing cyber threats, and hiring the talent (federal and otherwise) needed to execute their mission.

Despite increased workload and persistent challenges, CIOs and CISOs continue to find innovative ways to use technology to conduct the business of government faster and more efficiently. From increasing the use of Agile development to leveraging more advanced data analysis and management systems, from taking advantage of cloud-based solutions to utilizing different hiring and procurement strategies to integrate new ideas and energy into the workforce, CIOs and CISOs have never been more important in helping ensure the government is more responsive, nimble and cost effective.

TOP PRIORITIES

CIO TOP PRIORITIES

We begin our survey every year with an open-ended question to uncover the top priorities and challenges facing CIOs. The top priorities cited by survey participants this year were nearly identical to last year, including cybersecurity, IT modernization, the talent challenge, improving IT acquisition, and cloud.

CYBERSECURITY

It is no surprise that cybersecurity remains the top priority for CIOs. Protecting government information and networks from cybersecurity threats is, as one CIO described, a ***"never-ending bug hunt – we are constantly wondering what the bad guys are doing, whether they've done it to me and what I can do about it."*** And while successful intrusions into government systems continue to make headlines, overall, the government is making progress coordinating on cyber issues. CIOs felt like the "cyber sprint" conducted in the summer of 2015 was helpful for them to gain insights into their own cybersecurity risks and improve communication within the CIO community on threats and mitigations to common cybersecurity risks. One CIO said ***"the sprint led to agencies using combined brain power to address issues in cybersecurity."*** They agreed cybersecurity challenges will continue to be exacerbated as federal legacy systems and infrastructure age, and that additional investment is required to address this issue. They also stated hiring rules needed to change to make it easier to recruit and offer competitive pay to cybersecurity talent, of which they are in dire need.

IT MODERNIZATION

CIOs continued to emphasize the need to modernize legacy systems, reduce network footprints, rationalize and modernize applications, and migrate to the cloud. Modernizing the IT environment is needed to close security gaps, refresh infrastructure to improve IT performance, reduce spending on outdated equipment or software, take advantage of fast-changing technology improvements, and better manage, consolidate, and analyze the increasingly large volumes of government data. This problem will only get worse as time passes. As one CIO described, ***"we have 60M lines of COBOL and assembler code and over 30 percent of our IT staff are eligible for retirement in the next five years. It will be difficult to maintain these [systems in the future]."***

TALENT CHALLENGE

CIOs also identified recruiting and retaining talent as a top priority. Skills in greatest need include cybersecurity, Agile, cloud, and digital services. CIOs commented they lose top talent to one another as agencies compete for the best people, but also to the private sector, where pay is more lucrative. CIOs were in agreement that little progress has been made to make compensation for federal IT professionals more competitive. One CIO said, ***"why do certain agencies have special hiring authorities and pay rules? Is their mission more important than ours?"*** CIOs feel that special authorities and increased pay scales should be extended to all agencies, at least for certain skills like cybersecurity. CIOs agreed additional investment in training is needed to increase the technical skill level of employees and to help retain an experienced workforce.

IMPROVING IT ACQUISITION

CIOs are committed to working with their acquisition counterparts to reduce the time it takes to buy IT services and commodities, to better train IT staff in acquisition and acquisition staff in buying IT and to align IT acquisition with Agile development. One CIO said: ***"acquisition is too prescriptive."*** Another said, ***"the process offers innovative technology firms a disincentive to do business with us. It's too hard to get a vehicle in place, and they don't see a return on investment."*** This issue must be addressed by the next administration. Another CIO stated: ***"we don't have the quick agile contracting vehicles for us to do the work we need to do. Our agency is not open to using contract vehicles outside of their own and that can lead to protests. Course correction is difficult, and we need a change in culture."*** CIOs also explained they needed to improve at ***"writing contracts" and "training Contracting Officers and Contracting Officers Representatives on agile contracts."*** This is a perpetual challenge and something that desperately needs continued focus from both current agency leaders and the new administration.

MOVING TO THE CLOUD

Cloud migration remains one of federal CIOs' top priorities. As a community, CIOs continue to see benefits associated with cloud migration such as improved flexibility, faster application delivery, easier addition of services, improved customer service, and cost savings. But that migration does not seem to be occurring as quickly as CIOs would desire – only five percent of interviewees stated they are satisfied with the progress they have made in the cloud adoption process (down from eight percent last year).

CIOs identified a number of other priorities as well, including: successfully implementing FITARA, improving delivery of IT services in support of the mission, and improving transparency of IT spending and the return on investment for that spending.

ADVICE FOR THE NEXT ADMINISTRATION

CIOs are very positive about the work that has been accomplished, especially over the last year, including the Cybersecurity National Action Plan, making progress on FITARA implementation, creating a dialogue on how to fund legacy systems modernization, and improving how the federal government buys IT. As we move to the next administration, CIOs want to build on these accomplishments.

CIOs have a growing concern with cybersecurity threats and their agency's ability to respond in a timely manner. CIOs underscored the importance of reinforcing that cybersecurity is not solely an IT priority to be handled by the CIO, but must be coordinated and supported across the entire senior management team at agencies, including cabinet secretaries.

The need for speed, flexibility, and agility within the workforce and culture of agencies is also noted by CIOs. The new administration must find ways to better leverage technology to change the way agencies do business to respond more quickly and efficiently.

Survey participants also want incoming administration officials to fully consider on-going initiatives that will need continued support through the transition in order to be successfully implemented. These include but are not limited to FITARA, the Cybersecurity National Action Plan, legacy systems modernization, and streamlining the hiring process.

"Continued leadership from OMB on critical IT issues and challenges such as cybersecurity, talent challenge, and legacy system modernization."

"With an $80 Billion budget for IT there is plenty of room for optimization and elimination of redundancy across the board. The new administration should work with the Federal CIO Council to implement new solutions and approaches without reducing IT staffing."

"Recruiting and retaining highly qualified IT personnel is another top challenge that needs more attention. We are working with a complex hiring process, hiring freezes, gaps in competitive pay with the private sector, and the difficulty of locating individuals with the right skillsets and knowledge needed to transform and modernize the IT environment."

"Reduce duplication in commodity IT across agencies."

"Help CIOs find a way to better leverage technology to do our jobs better. The new administration should focus on bring innovative changes to the acquisition process (and culture) to create a better way to buy new technologies (Think big, start small)."

"Keep investing and modernizing. Need to get over that hump."

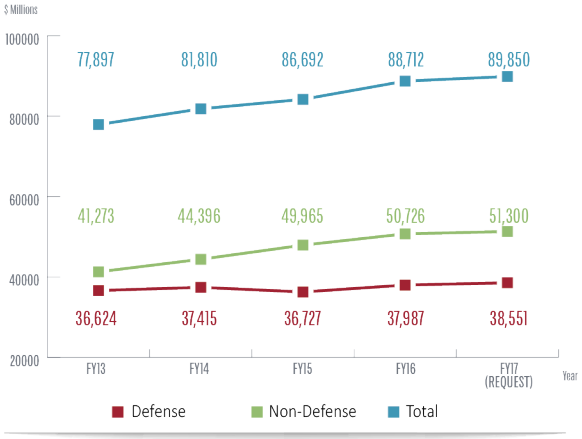
"Appointees should also be prepared to work in an uncertain budget climate while continuing to improve the quality of IT services, and drive down the cost of those services."

"Keep investing and modernizing agency systems"

FY2017 FEDERAL IT BUDGET PROPOSAL

The President's FY2017 budget request included a $1.14 Billion (1.3 percent) increase in total federal IT spending to $89.85 Billion. Growth was more evenly spread than previous years, with DoD IT spending growing $564 million (1.5 percent) and non-Defense IT spending growing $574 million (1.1 percent). These modest increases are in line with the trend during the Obama administration, where total IT spending has been held to a 1.8 percent compound annual growth rate since 2009.

FEDERAL IT SPENDING (IN MILLIONS)1

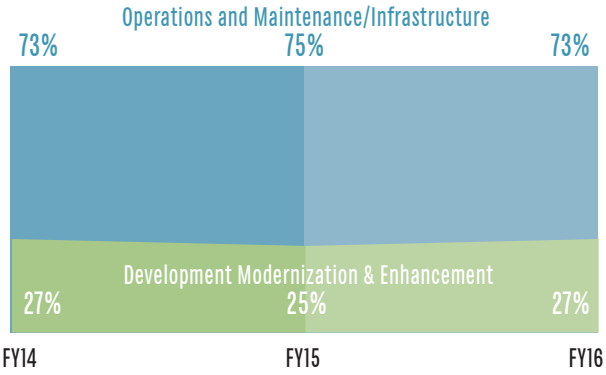


Source: Budget of the United States Government, Analytical Perspectives, FY 2015, FY 2016 and FY 2017

Each year, we ask CIOs and CISOs to provide their best estimate of the percent of spending they allocate to investing in development and modernization (DME) versus operations and maintenance (O&M) on legacy applications and infrastructure. While there was a strong recognition that agencies must reduce the funding spent on legacy systems and invest in new technology and solutions, in reality there is little change in the ratio reported by CIOs from the traditionally cited 25/75 percent split between DME and O&M.

Despite little movement in the overall ratio, there was some significant variation in selected agencies. One agency said it spent 90 percent on O&M and another said it had a mix of 40 percent DME and 60 percent O&M. Most CIOs however are not satisfied and are working very hard to restructure O&M spending to free up dollars to invest in new initiatives that improve efficiency, like cloud migration, digital services and the move to agile development. CIOs reported they hope to reduce the percentage of O&M spending at their agencies by an average of 10 percent over the next three years.

CIOs continue to see 73 cents of every dollar going to fund O&M



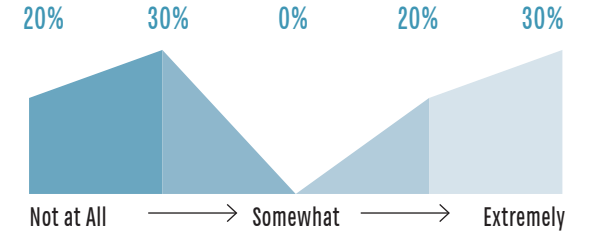
LEGACY SYSTEMS MODERNIZATION

Perhaps more important than the overall spending trends in this year's budget release, President Obama proposed to create a $3.1 Billion government-wide revolving fund to act as seed money to help modernize outdated IT systems across the government. The proposal would allow agencies to use the working capital fund to upgrade legacy IT systems that can be decades old. Since the budget was released, there have been bills introduced in Congress, most notably the MOVE IT Act, that would create working capital funds at individual agencies to accelerate modernization efforts, but that allocates no additional funds.

Reactions from CIOs to these new proposals have been mixed. Given the size of the Federal IT modernization challenge, some CIOs believe the $3.1 Billion IT modernization fund would have relatively little impact across government in helping agencies modernize legacy systems and improve cybersecurity. Other CIOs thought the fund would be useful for smaller

agencies where the dollar threshold for modernization projects is smaller. In addition, CIOs expressed reservations about the mechanism and ability to pay back money to the fund over time. Both legal requirements limiting the flexibility of funds appropriated to agencies to be used for other purposes and the potential for only limited savings to be achieved over time were mentioned as potential weaknesses in the revolving fund proposal. Regardless, all CIOs appreciate the dialogue and focus on this issue and agree more investment is needed.

How helpful would funding from the revolving fund for IT modernization be to your agency's modernization efforts?

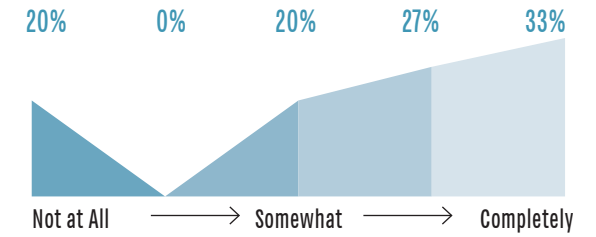


FITARA AND THE ROLE OF THE CIO

Since enacted in 2014, the Federal IT Acquisition Reform Act (FITARA) has demonstrated mixed results in its goal of transforming both the role of the CIO and how the government purchases information technology. This year's survey asked CIOs to comment on how FITARA has impacted them over the past year. CIOs of various agencies were mostly satisfied with their implementation of FITARA thus far and noted that it has been a catalyst for improving how agencies manage spending and purchases of IT. One CIO stated, ***"It has created a conversation – when you have people who are willing to work together it really does help. FITARA is an accelerator – it is mostly about the cultural change within your own agency. And at our agency it has helped the CIO get the information needed to make informed trade-offs."***

However, most stated it was still too soon to fully understand how their agency would utilize FITARA over the long term and if it would bring the transformative change that many supporters thought it would. Indeed, fully two-thirds of participants stated FITARA has had marginal to little impact on their agencies so far. CIOs feel FITARA has helped open up communications across management disciplines at agencies and in some agencies created better collaboration on IT investment and implementation decisions. Though agencies have made mixed progress, CIOs feel like FITARA will continue to provide them with a tool to improve how they invest in and modernize IT across the enterprise. One CIO stated, ***"The question of FITARA is not whether we should do it, it is how."***

CIO Satisfaction with FITARA Implementation



INNOVATION

TOP AREAS IN IT INNOVATION

CLOUD	APPLICATION MODERNIZATION	CYBERSECURITY	AGILE/DIGITAL

CIOs continue to find creative ways to innovate and bring new ideas into their organizations to improve IT service delivery. Some of the areas cited by CIOs where they are seeing the best results include crowd sourcing, application development, coding boot camps, the deployment of enhanced data access tools, the use of innovation labs, and the creation of mobile and digital services for employees, citizens, and other stakeholders.

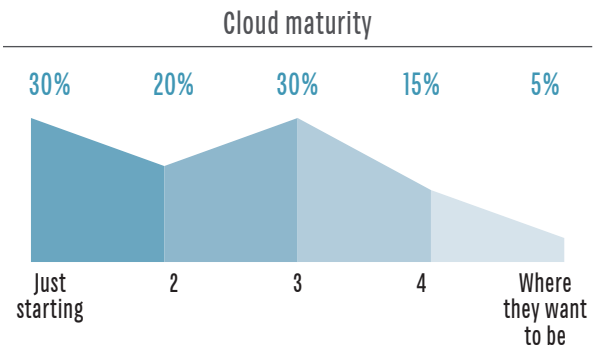
Like last year, CIOs said innovating can be challenging due to employee fears that trying something and failing will lead to being publicly chastised by an oversight body.

CLOUD

Almost six years after the release of OMB's Cloud First policy, and four years after the digital government strategy, federal CIOs report they continue to struggle with adoption of cloud technology with only five percent of interviewees stating they are satisfied with the progress they have made in cloud adoption (a decrease from the eight percent reported in 2015). One CIO remarked agencies need an understanding of architecture changes that must occur to identify what is most advantageous to move to the cloud while weighing cost effectiveness. Nonetheless, government agencies are actively evaluating their options and need to accelerate efforts to realize the benefits of commercial cloud solutions to address IT modernization, consolidation, and increased operational efficiencies.

In August of 2016, OMB released the Data Center Optimization Initiative (DCOI) policy, requiring agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure, such as cloud services and interagency shared services. By the end of FY2017, agencies will need to reduce physical data center costs by 25 percent overall, and close 25 percent of tiered and 60 percent of non-tiered data centers. This policy emphasizes "optimization" over "consolidation" because the efficiencies resulting from reduced costs and energy use may save more than $1 Billion over the next two years. By migrating infrastructure to the cloud, agencies are able to reduce their costs for data center hardware and software, licensing, and staffing.

In 2016, 33 percent of CIOs surveyed stated they had moved to the cloud in some capacity. One CIO explained their organization uses a hybrid cloud whereby the public cloud is used for public facing data and a private cloud is used for more sensitive data. For the agencies currently embracing cloud technology, email is commonly the first step to a bigger move toward advanced cloud technologies. Cloud adoption creates benefits for many agencies. CIOs noted one common benefit of cloud is the flexibility and scalability of a cloud solution. One respondent also stated, ***"The cloud is going to enable big data analytics and help rethink knowledge management."***



With a recognition of the opportunity to deploy "capabilities-as-a-service," some CIOs are exploring the idea of data as a service (DaaS). While the concerns surrounding DaaS are similar to those associated with cloud computing, the advantages of greater agility, cost-effectiveness and the potential for increased data make this option appealing to some.

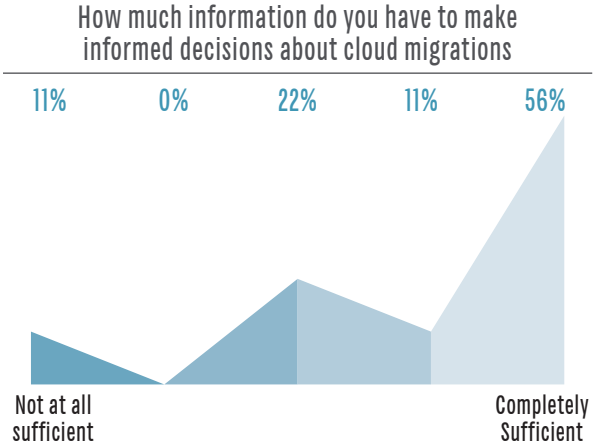
Some CIOs continue to report funding constraints as an obstacle to migration to the cloud. However, given the compelling value proposition of consumption-based buying, the significant continuing reliance on outdated infrastructure and the ability to quickly repurpose operations and maintenance funding, the need and opportunity has never been greater to move more rapidly to the cloud.

Some CIOs identified other issues surrounding cloud adoption. As one CIO stated ***"my main concerns are security, interoperability and the network."*** Those pain points are echoed throughout the federal government among other concerns such as data security, third party vendors, and staff that understand cloud and cloud architecture. Despite significant security concerns with outdated government infrastructure, migration to the cloud still drags at a slow rate.

A number of CIOs note lessons learned from cloud implementations, stating, ***"The challenge is to ensure agencies take on the responsibilities they have for risk management and not turn it over to the cloud provider."***

Another interviewee explained getting the right people with experience in cloud is imperative to success.

Despite numerous examples of successful cloud migration, some IT leaders are still hesitant to move forward. CIOs feel like they are more educated around how to move now than in previous years.



Our 2016 CIO Survey respondents describe the transition away from existing data centers to the cloud as "a mindset issue." Despite plenty of low-hanging fruit ready to migrate, agencies have been slow in making progress.

Cloud Lessons Learned

- Ensure agencies take on the responsibilities for risk management and not turn it over to the cloud provider.
- Need transparency of security perimeters through items like data logs.
- Need to have maturity in architecture and data knowledge to know what can and cannot go into the cloud
- Take the time to develop a detailed plan with a phased approach to migration
- Mature migration processes and architectures before moving into a cloud architecture
- Ability to negotiate effective contracts so we are only buying what is needed and do not get locked into poor contracts.

Thoughts on FedRAMP

The implementation of The Federal Risk and Authorization Management Program (FedRAMP) in 2014 was intended to help alleviate some cloud technology security concerns and accelerate the adoption of secure commercial solutions, but some CIOs remain concerned about the effectiveness of this effort. One CIO shared frustration with this government-wide program providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services, saying the whole process takes too long. Another interviewee cited similar frustrations with burdensome requirements for solutions that only house low-risk data. One CIO had a differing opinion and cited the use of FedRAMP–approved solutions to host data without any major setbacks. Although steps are being taken to streamline the FedRAMP process, the lack of reciprocity (requiring agencies to rely on another agency's ATO or provisional authorization) must be addressed to accelerate the adoption of commercial cloud solutions.

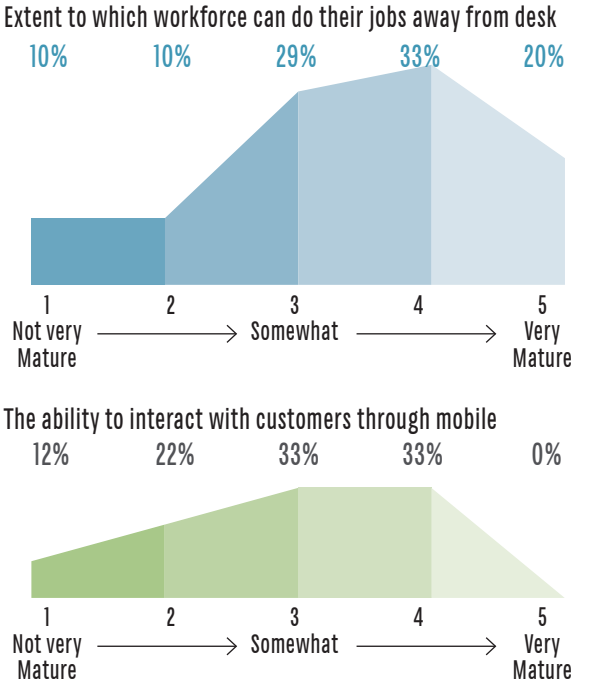
MOBILITY

According to comScore,[1] a global media measurement and analytics company, smartphones and tablets are now outpacing the use of laptops. Mobile now represents 65 percent of digital media time, while the desktop is becoming a secondary source for digital users. Although the federal government has been slow in adopting and integrating mobility into their IT infrastructure, it is not surprising that agencies are evolving to keep up with this new paradigm.

When asked about their agency's mobile maturity– defined as the ability for employees to work remotely– CIOs had a variety of answers from not using mobile technology to the ability to complete virtually all work remotely. Indeed, current federal agency ability to interact with citizens and other stakeholders through mobile platforms has not matured much in the last year. CIOs want to improve their ability to interact with their customers through digital platforms. Agencies are investing more in digital services and creating internal digital services teams. One CIO stated, ***"implementation has been bumpy but we are glad it's being done."***

For those respondents citing a high level of mobile maturity, government furnished equipment – primarily laptops – are still the most common devices deployed.

Organization's mobile maturity



An agency's mobile maturity impacts a wide range of issues, particularly federal employees' ability to work from locations other than the office. This has an impact on each employee's flexibility and productivity, but perhaps more importantly has a direct connection to an agency's ability to operate during a disaster or other emergency. One CIO stated, ***"On any given day, 50 percent of the workforce is teleworking, with that number jumping [at times] to 80 percent... The number of desktops has gone almost to zero as all staff now receive laptops."*** Many CIOs explain the next phase of increasing mobility is ensuring employees use the various mobile capabilities currently in place. ***"We have tons of mobility, it's a matter of all personnel using it,"*** explained one CIO.

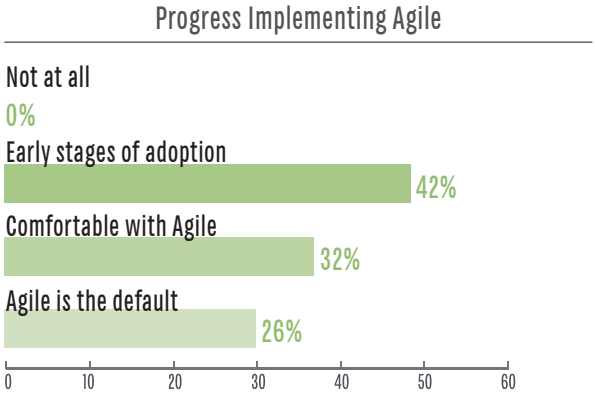
This is more than just a technology issue, as it has an impact on employee morale and efficiency of operations at agencies. Those agencies that provide employees with mobile devices, telework schedules, and mobile apps are ranked higher among the best places to work.[2] Maintaining telework technologies and polices is imperative to attracting and retaining talent. Although not all agencies stated a need for mobile applications, one CIO explained the agency is committed to making everything mobile and accessible including the capability for employees to use their own technology ("Bring Your Own Device").

Those who are not yet mobile cite reasons such as security restrictions, legacy hardware, counterparts not being mobile, and collaboration issues as obstacles to adoption of mobile solutions. One CIO explained that although they are not where they want to be in the realm of mobility, work is being done to build cross-domain capabilities, which while expensive, can help to mitigate issues around security restrictions.

In today's world where federal employees often have better personal mobile devices than those offered by their employer, and with the need for employees to be connected anywhere/anytime, the mandate to be able to do trusted computing from untrusted devices must be addressed.

ADOPTING AGILE DELIVERY IN A NON-AGILE ENVIRONMENT

Adoption of Agile methodologies for delivering IT projects continues to gain traction across the federal government. This year every interviewee stated they are using Agile in some way, compared to 9 percent who said they were not using it last year. The number of respondents using Agile as the default increased from 26 to 33 percent. CIOs are moving to DevOps and integrated testing and using time boxed Agile across several platforms. CIOs report Agile has helped improve customer service and engagement and sped delivery of value to customer.



But there remain significant barriers to the adoption of agile at many agencies. One CIO mentioned their current efforts to expand the understanding of basic components of Agile across their entire agency – not just within IT development teams. ***"We are working to disseminate these practices and methodologies across the entire culture instead of just parts of it."***

In addition, CIOs are struggling to integrate Agile throughout their organizations - from IT delivery teams to the business side.

"I like to think agile is the default but our agency has limited readiness for Agile. We need to further develop processes and train people in how to do Agile. Many groups not comfortable with Agile." Respondents also cited they continue to have a difficult time setting up the right metrics to evaluate the effectiveness of their Agile implementations, hiring qualified Agile staff, and creating efficient approaches to budgeting for and buying Agile services.

Despite an increased use of Agile, CIOs and other IT executives continue to struggle with managing large IT projects and programs. One CIO stated the federal government does not deliver large enterprise programs well and that there needs to be proper steps in place to not have those projects fail from the start. Others are frustrated with the lack of a modular approach and the continued emphasis on enormous IT projects. ***"There is a history of having large federal IT programs, where $100M would not be considered big, and that mindset needs to go away,"*** stated one CIO.

Large federal IT projects are notorious for delays and implementation challenges, and the magnitude of cultural change needed at an agency is often underestimated. Other common challenges mentioned during the survey interviews centered on coordination across the project teams and stakeholders – particularly integrating input and feedback from business owners. CIOs spoke of an inability to oversee and communicate requirements and progress on large scale IT projects and a lack of certified and experienced project managers as key aspects that can lead to failure of a project. Almost all the CIOs surveyed agreed large-scale federal IT programs are often fraught with risks and extremely difficult to implement.

One way CIOs are managing the risk of their IT projects is continual program and risk evaluation. They believe having transparency at all levels will make it easier for projects to succeed. One respondent reported their executive team sees project performance updates for one particular large IT investment every week and has regular weekly management reviews to make decisions to modify/adapt program goals/requirements to ensure the project's success. Another respondent believed having the right metrics to measure the success of the project was crucial and that these metrics must be tied to customer satisfaction. Yet even with management buy-in and clear performance indicators, many CIOs still stressed the importance of communication. One CIO stated,

> "When considering the structure of your team on an IT project, it is crucial to have a dedicated communications person – most teams focus solely on project and delivery."

One way to prevent failed IT projects is to break the large projects into smaller ones. Using a modular approach reduces the risk associated with a large project and allows agile methods to be used more effectively. There are still obstacles, however, to aligning financial management and acquisition processes to support an Agile delivery model. Without this alignment, it can be difficult to move away from large

scale implementations to modular/agile development and realize the full potential of Agile methods.

A second practice highlighted by CIOs that can help prevent future project failures is being more transparent about why projects fail. This can help other agencies avoid similar mistakes in the future. The lessons learned from project failures should be documented and shared with other agencies – especially those with similar missions or IT implementations. Lastly, attracting more experienced program managers to run IT projects was a key differentiator for CIOs.

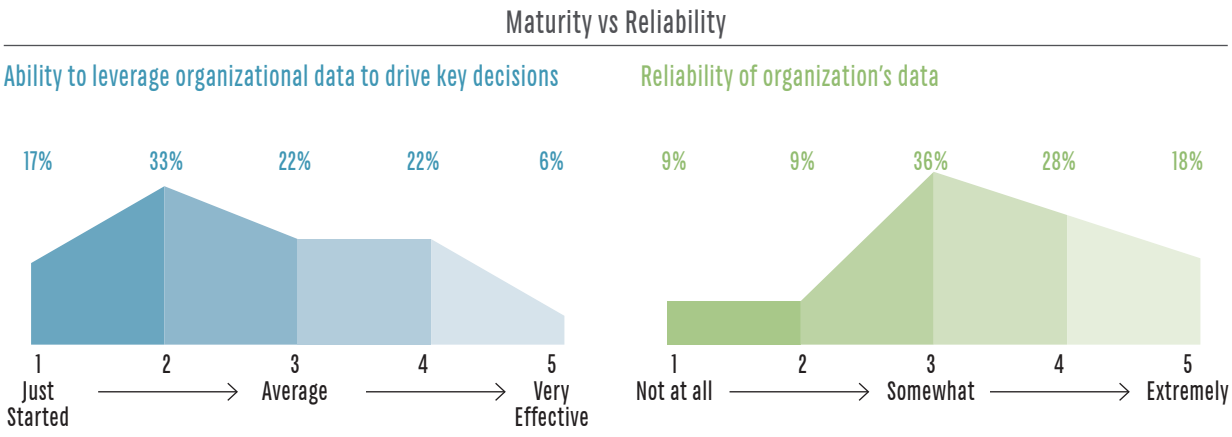
DATA MANAGEMENT AND ANALYTICS

Data management in the public sector continues to be an area of focus, with evolving attention from data warehousing to modernizing enterprise data platforms, and advancing analytics programs to drive decisions across lines of business. To lead these developments, a number of federal agencies are appointing a Chief Data Officer (CDO) to be in charge of coordinating the data strategy. The vast majority of executives (86 percent) who responded to the survey confirmed having a CDO at their agency this year and had positive expectations about the new role.

There remains a substantial variation in levels of data management maturity in the federal government. Similar to last year's survey results, a majority of respondents indicated their agencies' data-driven capabilities were still in the early stages of maturity, with 72 percent of respondents describing their organization's ability to use data to drive key decisions somewhere between immature to somewhat developed. Agencies continue to report that this limitation is not due to a lack of data, but rather about managing and drawing meaningful insights out of the data the agency is currently maintaining. We also asked CIOs to comment on the reliability of their data, and like last year, 45 percent of agencies rated their data as very reliable.

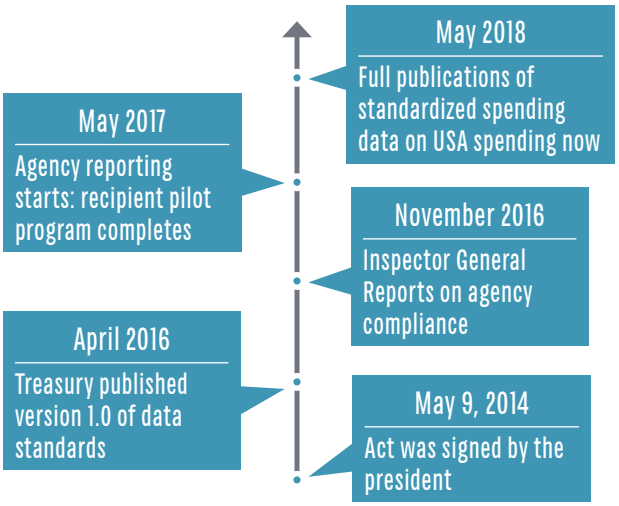
Respondents point to difficulty with the IT acquisition process as a common challenge affecting the maturation of their data management programs. Agencies with a "decentralized" approach to generating IT program requirements describe a lack of transparency and collaboration for determining data management solutions that will be effective on an enterprise level. CIOs also indicated they want to improve the way their organizations use data to drive key business decisions, and support centralizing IT acquisition, data governance, and enterprise data management to strengthen mission-oriented analytics activities. Agencies are also responding to financial pressures to streamline, automate, and consolidate technology. This includes combining redundant efforts and modernizing to lower-burden, higher-efficiency data management tools.

This year also saw agencies implementing the Digital Accountability and Transparency (DATA) Act, bringing increased scrutiny to spending data transparency and reliability. Agencies still struggle to accurately report on operational performance, particularly at an enterprise level. Though the DATA Act requires agencies and federal entities to self-identify whether they are required to comply with the mandate, a recent GAO report found that, as of July 2016, Treasury and OMB



did not have a definitive list of those agencies. The levels of involvement and committed resources to prepare and comply with the DATA Act varies across agencies. The GAO report reviewed 42 implementation plans submitted by different agencies and that none contained all required elements. We can expect more focus on DATA Act implementation through the spring of 2017 as the deadline for agencies to report to Treasury approaches. The CIO with support from their CDO will play a key role in creating the data governance strategy and implementing the technology solution needed to enable their agencies to meet the mandate of the DATA Act. One CIO said, ***"It is our role to ensure the data is accessible and secure."***

Data Act Timeline



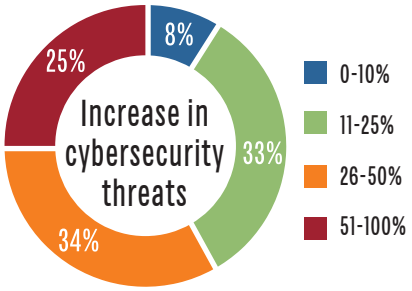
CYBERSECURITY

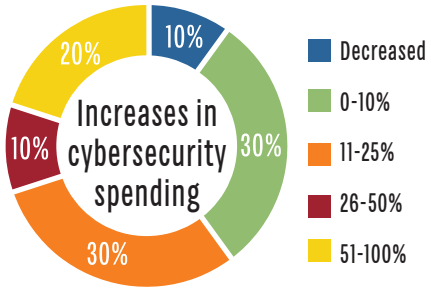
The 2016 World Economic Forum Global Risk Report[3] identified cyber attacks as one of its top risks in both likelihood and impact for the third straight year. An estimated $373 Billion to $575 Billion in damages are attributed to security breaches in the U.S. alone. It is no surprise that cybersecurity remains the top priority and challenge for CIOs and CISOs in the federal government. Socially engineered spam, phishing, spyware and other external threats from cyber criminals, nation states, and rogue actors are more sophisticated and persistent than ever. CIOs and CISOs must also be aware of and manage internal threats from staff who unintentionally create risks from forgotten passwords, prohibited downloads, or lost devices.

One of our interviewees stated, ***"The biggest information security challenge is keeping data secure while still remaining collaborative; being able to share and work with others without compromising security."*** The traditional methods of boundary protection are no longer sufficient. Cybersecurity must address verifying risks from multiple threat vectors across a multitude of networks and devices inside and outside an agency.

Not only is cybersecurity a top risk for federal CIOs, but attacks and the type of threats are getting more frequent. Over half of CIOs and CISOs reported threats to their agency have increased by at least 25 percent in the last year. Thirty-four percent of CIOs surveyed experienced an increase in cyber incidents in the past two years. Over 40 percent reported an increase in mobile computing cyber threats. A number of CIOs believe the increase in threats could be due in large part to social engineering and phishing, all of which could be helped significantly by better training and awareness. Lastly, lost time and productivity were reported as a key impact to the organization due to security breaches.

Changes in Cybersecurity Threats & Spending





"Security is a function of culture and behavior - technology will not solve the issue of an agency being at risk"

Cybersecurity spending is increasing too, but not proportionally to the increase in threats. Approximately half of CIOs cited a moderate increase of between zero and 25 percent in cybersecurity funding, with only 10 percent reporting a decrease. This is an improvement over last year in which only 15 percent of agencies reported a zero - 25 percent increase in cybersecurity funding. One of the main concerns voiced by the CIOs is making cybersecurity spending a priority and not an add-on cost. Also, some agencies had difficulty separating general IT and cybersecurity costs. Currently, less than 40 percent of CIOs reported their organization having an effective information risk management strategy.

A huge concern echoed by the CIOs in this year's survey was attracting and retaining top-tier security and privacy talent. According to a report[4] from National Cybersecurity Alliance released last October, in 2014, U.S. companies posted 49,493 jobs that require Certified Information Systems Security Professional (CISSP) certifications. However, only 65,362 people are CISSP certified in total, and most of them already have jobs.

CIOs and CISOs feel the federal government has difficulty attracting top talent because of limits on compensation and the length of the hiring process. Specifically, they said it was almost impossible to compete with the commercial sector, which can offer more lucrative salaries with bonuses and can make offers faster than government. Another concern voiced by respondents is the risk of developing individuals and then losing them to industry or other agencies that have special hiring authorities and can pay more. Retaining top government cybersecurity experts can be impeded by lack of training funds and opportunities at some agencies, according to one CIO.

Despite the frustrations that came across in the survey, there has been some progress on hiring more cybersecurity professionals in the government. Beth Cobert, the Acting Director of the Office of Personnel Management, announced in a speech in late August that the government had hired twice as many cybersecurity professionals this year as compared to last year[#]. This increased hiring trend will hopefully continue due to the release of the Federal Cybersecurity Workforce Strategy, which outlined a series of near-term actions to eliminate the cybersecurity workforce shortage.

CONTINUOUS DIAGNOSTICS AND MITIGATION

Many of the respondents said they were using the Continuous Diagnostics and Mitigation (CDM) program for their continuous monitoring needs. Of those utilizing the program, three-fourths said it has had a positive impact on their ability to protect data and networks. As a part of that program, respondents stressed the importance of replacing or significantly curtailing the every three year paper assessment process of information systems required under FISMA and the FISMA Modernization Act. This old process is inefficient, results in out-of-date security information and ultimately increases risk for agencies by pulling personnel and resources away from higher priority investments in cybersecurity.

"This program helps to move us in the right direction from paper-based compliance to more real-time automated monitoring and response capability, placing us in a better position to respond quickly to federal cyber events."

In July 2016, The Office of Management and Budget released A-130, which moves from the requirement to re-evaluate security systems every three years toward a continuous monitoring approach. Unfortunately, Inspectors General (IGs), who are charged with overseeing agency compliance with FISMA and the old paper accreditation process, are still bound to conduct reviews of how well agencies are complying with the law. There has been significant discussion between IT executives and IGs and among IGs through the Council of the Inspectors General on Integrity and Efficiency about the proper approach to balancing more effective cybersecurity programs like CDM with outdated statutory mandates still in effect in laws like FISMA.

Over the next year, CIOs expect the CDM program to have a greater impact as it becomes fully operational with a federal dashboard and additional services, such as automated assessments, up-to-date information/data and immediate vulnerability detection and remediation. One CIO stated, ***"[CDM] should expand capabilities, deploy more quickly, and fund the tools beyond a year or two."***

ACQUISITION/INVESTMENT MANAGEMENT

CIOs and CISOs continued to report significant challenges with the federal acquisition process. Specifically survey respondents this year cited long lead times, a lack of agile acquisition solutions, challenges in requirements development and poor training options available to acquisition professionals in buying IT or using agile and non-acquisition staff who work with procurements. These challenges are exacerbated by the rapid pace of both technology and operational environment changes.

> "In acquisition it's each program for itself and there is no way to bring it all together."

One interviewee said they are trying to break procurements up into smaller actions in an attempt to shorten the acquisition timeline. Many interviewees also voiced concerns that even once they are able to get a contract in place, the current process is not agile enough for a rapidly changing IT environment. It is the general perception the Federal Acquisition Register (FAR) needs to be changed to make IT acquisitions solutions more agile. In reality, current flexibilities that already exist in the FAR are often not used. Managed services, performance-based contracts, statements of objectives, preferring commercial solutions, and encouraging alternative proposals can all help to improve acquisition outcomes.

The final major challenge mentioned is a need for training of contracting officers, CORs and CIO personnel. The changing nature of IT acquisitions and the growing reliance on buying "capabilities-as-a-service" require new skills and expertise. The government recognizes these training challenges and attempts are being made to remedy this gap, for example, through the Department of Defenses' additional guidance for services acquisitions released in early 2016. However, this guidance still needs substantive work to streamline the process and deliver better outcomes. The acquisition community is also challenged in buying IT and is in need of training in IT–specific disciplines such as agile acquisitions, DevOps, and cybersecurity.

Respondents viewed Lowest Price Technically Accepted (LPTA) acquisition strategies as a problem that drives out reasonable offerers. One interviewee stated ***"The acquisition community is highly motivated to achieve its goals, so yes it is being used and it is a frustration across the industry. LPTA is proving to drive responsible vendors out and we're trying to drive back to a best value. We recognize this is an issue. The motto is cost focused and not mission focused as it should be. There needs to be collaboration on how to resolve these problems."*** Agencies recognize this as an issue and are trying to change the focus back to best value. Respondents agree LPTA is a tool that should be used only when it is appropriate. One interview noted, ***"the challenge is, how do you evaluate these contracts to come to the right conclusion?"*** This appears to align with past years' interviews and the concern that the use of LPTA is an inappropriate approach to procuring IT services. The public sector is currently seeing the problems associated with the excessive or inappropriate use of LPTA, including protests submitted prior to award.

PAIN POINTS IN IT ACQUISITION

EDUCATION

- Insufficient education of acquisition specialists and general counsels in IT buying
- IT staff has limited education in procurement and legal processes
- Rigid interpretation of the rules by legal and procurement
- Misunderstanding of when contracts and program staff can interact and meet with vendors

RULES

- Vendor protests are too easy and fear of protests extend acquisitions
- LPTA produces poor results and costs more in the long run
- Requirements to award to small business can limit ability to get the right skillsets
- Simplified acquisition threshold is too low

PROCESS

- Misalignment between procurement rules and agile development
- Difficulty sharing contracts across agencies
- Siloed buying process; too many handoffs between program, IT, acquisition, legal
- Lack of analytics to guide buying

IT SHARED SERVICES

As in past surveys, the vast majority of CIOs and CISOs report they are using some form of shared service or have plans to move to a shared service in the near future. Despite that common response, almost every CIO/CISO said they are only adopting a shared services approach "where appropriate," a fairly significant caveat considering some of the current government-wide mandates to move to existing government-wide shared services like payroll and financial management providers. Overall, CIOs/CISOs are adopting shared services to help reduce duplication and increase efficiencies within their common support services.

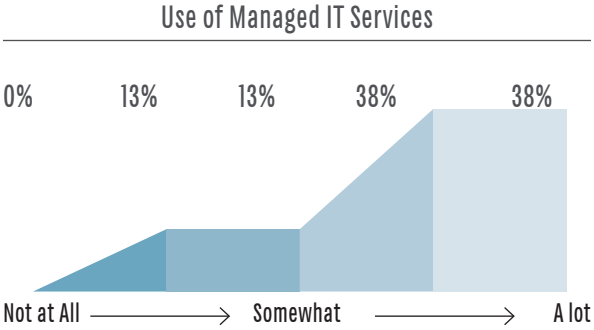
Despite the uniformity in responses about using some type of shared service, the type of model being used varies from department to department and CIO to CIO. Some are making use of government-wide shared services, like payroll, travel, and financial management services, while other respondents reported they have been building an intra-agency shared services model and allowing certain bureaus or components to be the provider for particular services that are sold to others within the same agency.

Regardless of the type of model being implemented, the main focus across the government is on "commodity" IT shared services – the more traditional back office functions like email, voice communications and help desk support – rather than on mission facing systems. Perhaps one exception to that theme is the adoption and use of services provided by DHS under the Continuous Diagnostics and Mitigation program.

This trend mirrors the initial focus of a new office at the General Services Administration – the Unified Shared Services Management (USSM) office. It was created in October 2015 to oversee the current shared services ecosystem and provide integration, communication, and collaboration support between agency customers and government shared service providers. The office's initial focus is on shared services in the traditional management areas of financial management, human resources, acquisition, information technology, and grants management. According to CIOs we interviewed, it is still too early to know whether the USSM office is making a difference in helping agencies adopt shared services that deliver quality products and services.

CIOs/CISOs also shared lessons learned and advice for their colleagues regarding moving to a shared service environment. The most common response was on the need for engagement and frequent communication between customers and service providers in order to communicate expectations and understand performance, particularly before deciding to move to a new provider. They also stressed the importance of having appropriate Service Level Agreements that clearly spell out those performance benchmarks and expectations and training for government staff, who may be particularly inexperienced with shared service models.

These lessons learned and pieces of advice are important in order to ensure quality and meet service expectations. Some respondents felt that government shared services are not often the best product or quality of service even if they are lower cost. And the lack of a penalty for poor services/support from a government shared service provider is inhibiting some CIOs/CISOs from more fully supporting transitioning systems or services to a government shared service provider. One CIO remarked, ***"If shared services are done right, there would be a consequence for not delivering."***



TALENT CHALLENGE

Recruiting, retaining and developing a workforce with the needed competencies and skills is a constant challenge in any organization, but particularly in the federal government, which faces unique challenges. ***"The greatest challenge for federal agencies is recruiting and retaining younger employees, those who represent the foundation of the workforce in the years ahead."*** As the government workforce continues to age (the average federal worker is now over 45 years old – more than three years older than the average private sector worker) and retirements put pressure on agencies to retain the knowledge and know-how to continue effective performance and service delivery, these challenges will only grow.

A recent study by the Partnership for Public Service found that while workers under the age of 30, (a majority of the Millennial composition) make up 23 percent of the overall U.S. workforce, "Millennials now comprise only 6.6 percent of the federal workforce, compared to 9.1 percent as recently as 2010 and the fewest since 2005."[5] In addition, over half of federal employees are Baby Boomers (aged 45-64) and are rapidly approaching retirement. These demographics foretell a government in danger of losing deep experience and institutional memory over the coming decades, endangering the performance of government programs and services. These sentiments were shared by many of the CIOs and CISOs who participated in this year's survey, and yet, respondents continued to echo similar messages as in past surveys about the obstacles and challenges that remain in developing a future-ready workforce. CIOs and CISOs identified a number of challenges they need to overcome, including accessing the hiring flexibilities needed to attract new types of talent and bring them on board quickly, translating current tech skills and needs into OPM's antiquated workforce nomenclature, paying competitive rates to attract the top tech talent – particularly in the area of cybersecurity – and figuring out how to either re-train or shift to other positions members of an aging workforce who no longer have relevant skills. Some of the talent gaps continuously mentioned throughout this year's interviews were in the areas of:

- Cybersecurity Talent
- Digital/Mobile Services
- Architecture
- Agile/DevOps

Multiple respondents in the survey reported an inability to find candidates for positions who could think on their feet, engage in problem solving, and could communicate effectively – basic professional skills needed not just in IT positions but across all job types. A discouraging insight given the high caliber of new employees taking jobs in the private sector. In fact, 86 percent of survey respondents have only a moderate level of confidence in their agency's ability to support their talent development needs.

Many agencies were interested in using new, more direct approaches to attracting younger, tech-savvy workers to government service, but often felt blocked by bureaucratic rules and onerous process requirements. The result is that even if top talent is interested in working in government, they are either lured away by higher salaries in the private sector or grow frustrated by hiring cycles than can last up to 9-12 months. Some agencies have had success in this area, including the U.S. Digital Service, Presidential Innovation Fellows program, and 18F at GSA, by marketing government tech jobs directly to Silicon Valley and other tech hot spots. But most evidence suggests these gains have been on the periphery and that the majority of tech talent continues to be hired through traditional channels rather than targeted outreach.

CIOs had a few suggestions for addressing talent challenges. First, extend current hiring authorities granted to a few agencies government-wide so all CIOs can utilize them. Second, invest more dedicated resources in IT training and certifications. And third, inject new funds to allow government to come closer to competing with compensation packages offered in the private sector.

THE BALANCE BETWEEN CONTRACTORS AND FEDERAL EMPLOYEES IN THE IT WORKFORCE

Last year we reported the estimated balance between federal and contractor employees was tipped in the direction of contractors by 22 percent with the intent to close this gap to 2 percent by 2020. This year we asked our participants how much agencies have been able to close the gap in the past year. The responses provided indicate agencies are relying more on the federal workforce, rather than contractors, to meet their IT needs. However, this year participants also indicated the four year forecast needed to be readjusted as the government continues to address challenges within the federal workforce such as compensation, the hiring process, and retaining staff. As a result, the four year projection has slightly increased from a 2 percent difference between federal and contractor employees to 6 percent.

	2015		2016	
	Federal	Contractors	Federal	Contractors
What is the balance between federal employees and contractors in your organization now?	39%	61%	43%	57%
In the next 4 years, what do you anticipate the balance to be?	49%	51%	47%	53%

CONCLUSIONS

In this year's 26th anniversary survey, it remains clear federal information technology leaders are in the spotlight more than ever. Their work is integral to every mission and function in government and expectations run high to both reduce operational costs through the use of technology while simultaneously bringing new, innovative solutions to government.

The focus on IT modernization and enhanced cybersecurity will be relentless. CIOs and CISOs will not only need to continue to push hard to implement these important efforts, but also must be savvy at navigating the transition to a new administration in the months ahead. To a person, all of the federal CIOs and CISOs interviewed for this survey both recognize this imperative and are up to the challenge.

The stakes are high. The federal government is at an inflection point. By focusing on the top priorities outlined in this survey, current federal IT leaders and those to come during the next administration will dramatically improve mission effectiveness and service to the citizens of this nation. Together, we are confident that with continued investment, creativity, and risk taking, we can build a more efficient and effective federal technology environment.

References

[1] "2016 U.S.Cross-Platform Future in Focus." comScore White Paper. March 30, 2016. Web. <http://www.comscore.com/Insights/Presentations-and-Whitepapers/2016/2016-US-Cross-Platform-Future-in-Focus>

[2] "Best Places to Work in Federal Government." Partnership for Public Service. 2016. Web. <http://bestplacestowork.org/BPTW/>

[3] "The Global Risks Report 2016." World Economic Forum. January 14, 2016. Web. <https://www.weforum.org/reports/the-global-risks-report-2016>

[4] "Securing our Future: Closing the Cybersecurity Talent Gap." National Cybersecurity Alliance. October, 2015. Web. <https://staysafeonline.org/download/datasets/16847/Securing%20Our%20Future%20Closing%20the%20Cybersecurity%20Talent%20Gap.pdf>

[5] "Improving the Employee Experience: What agencies and leaders can do to manage talent better. " Partnership for Public Service. August, 2015. Web. <http://ourpublicservice.org/publications/download.php?id=556>

APPENDIX A – LIST OF INTERVIEWEES

JONATHAN ALBOUM
Chief Information Officer
Department of Agriculture

DARREN ASH
Chief Information Officer and Division Director
Farm Service Agency
Department of Agriculture

DOUG BAILEY
Deputy Administrator and Chief Information Officer
Agricultural Marketing Service
Department of Agriculture

KRISTEN BALDWIN
Deputy Chief Information Officer
Department of Transportation

MIKE BARTELL
Chief Information Officer
Information Technology Services Division
Oak Ridge (TN) National Laboratory
Department of Energy

LT. GEN WILLIAM BENDER
Chief, Information Dominance and Chief Information Officer, A6 Office of Information Dominance and Chief Information Officer [SAF/XC]
Vice Chief of Staff
Department of the Air Force

GORDON BITKO
Chief Information Officer, ITB
Federal Bureau of Investigation
Department of Justice

SYLVIA BURNS
Chief Information Officer
Department of the Interior

PHILIP CLARK
OST Chief Information Officer
Department of Transportation

STEVE COOPER
Chief Information Officer
Department of Commerce

SCOTT CORY
Director of Information Resources Management and Chief Information Officer
Administration for Community Living
Department of Health and Human Services

KEVIN DEELEY
Deputy Chief Information Officer
Department of Justice

DAVE DEVRIES
Principal Deputy Chief Information Officer
Office of the Chief Information Officer
Department of Defense

DEBORAH DIAZ
Deputy Chief Information Officer and Chief Technology Officer for Information Technology
National Aeronautics and Space Administration

JUDITH DUDLEY
Acting Deputy Administrator & Chief Information Officer
Agricultural Marketing Service
Department of Agriculture

ANN DUNKIN
Chief Information Officer and Assistant Administrator for Environmental Information
Environmental Protection Agency

DR. STEVEN FINE
Principal Deputy Assistant Administrator
Assistant Administrator for Environmental Information
Environmental Protection Agency

ROB FOSTER
Chief Information Officer
Department of the Navy

ADRIAN GARDNER
Director and Chief Information Officer
Federal Emergency Management Agency
Department of Homeland Security

JOSEPH GIOELI
Acting Chief Information Officer
United States Mint

ZACH GOLDSTEIN
Chief Information Officer
National Oceanic and Atmospheric Administration
Department of Commerce

MARGIE GRAVES
Deputy Administrator and Deputy Federal Chief Information Officer (Acting)
Office of Management and Budget

GEORGE JAKABCIN
Chief Information Officer
Treasury Inspector General for Tax Administration
Department of the Treasury

STAN KACZMARCZYK
Director of Cloud Computing
Cloud Computing Program Management Office
General Services Administration

JOSEPH KLIMAVICZ
Chief Information Officer
Department of Justice
Department of Homeland Security

MICHAEL KLOPP
Acting Assistant Director
IT Customer Relationship and Management Division
Federal Bureau of Investigation
Department of Justice

ROBERT KLOPP
Chief Information Officer
Social Security Administration

MARK KNEIDINGER
Director, Federal Network Resilience Division
Office of Cybersecurity and Communications
Department of Homeland Security

JAY MAHANAND
Chief Information Officer
U.S Agency for International Development

RICHARD MCKINNEY
Chief Information Officer
Department of Transportation

CAROL MULLINS
Associate Commissioner
Office of Technology and Survey Processing
Bureau of Labor Statistics
Department of Labor

KEVIN NALLY
Chief Information Officer
Office of Technical Development and Mission Support
Secret Service
Department of Homeland Security

JOE PAIVA
Chief Information Officer
International Trade Administration
Department of Commerce

DR. RON ROSS
Senior Computer Scientist and Information Security Researcher
National Institute of Standards and Technology

LISA SCHLOSSER
Acting Chief Information Officer,
Office of Personnel Management

CHAD SHERIDAN
Chief Information Officer
Risk Management Agency
Farm and Foreign Agricultural Services
Department of Agriculture

TODD SIMPSON
Chief Information Officer
Food and Drug Administration
Department of Health and Human Services

HERB STRAUSS
Assistant Deputy Commissioner and Deputy Chief Information Officer
Social Security Administration

MINH-HAI TRAN-LAM
Acting Deputy CIO
Department of State

STEPHEN WARREN
Chief Information Officer
Office of the Comptroller of the Currency
Department of the Treasury

RICHARD YOUNG
Chief Information Officer and Associate Chief Operating Officer
Foreign Agricultural Service
Department of Agriculture

APPENDIX B – LIST OF INTERVIEWERS

PSC

DAVID M. WENNERGREN

DONALD BAUMGART

MICHELLE JOBSE

GRANT THORNTON SURVEY TEAM

GEORGE DELPRETE

ADAM HUGHES

MICHELLE MONTOYA

GLORIA FUNES

CIO INTERVIEWERS

MELANIE ANGE
CenturyLink

NOREEN AVANCENA
Cisco

AURPON BHATTACHARYA
Grant Thornton

EDWARD BLISS
Grant Thornton

BENITA BOTTON
Business InfoStrategies

MICHAEL BRUCE
General Dynamic Mission Systems

ROBERT BURNHAM
Grant Thornton

CHRIS CAMPBELL
Grant Thornton

ALVARO CASTILLO
Unisys

DIANE CEBAN
SAIC

TOM CHAR
Grant Thornton

MARYELLEN CONDON
Condon Associates LLC

MICHAEL COWENS
Maximus

SANDRA CUNNINGHAM
Grant Thornton

JENSON DANIEL
Organon Advisors

ASIA DAWSON
Heitech Services

GIOVANNINA DIPIETRO
Optum Federal Solutions

CHARMAINE EDWARDS
Microsoft

AMY FADIDA
A.M Fadida Consulting

JIM GAUL
Accenture Federal Services

RICHARD GIEBEL
AT&T Government Solutions

BRENDA GIROD
ICF International

DONNA GLASSLEY
SAIC

DERRY GOBERDHANSINGH
e3 Federal Solutions

GAYLE GRASSO
IBM

ROBERT HAAS
Hewlett Packard Enterprise

JOHN HAMILTON
AT&T

SCOTT HEEFNER
Information International Associates, Inc.

KRISTIN HUG
DRT Strategies

TRICIA IVESON
10novate

KATHERINE JACKSON
Grant Thornton

JEFF JOHNSON
Grant Thornton

SHEREE JONES
IBM

STEVEN KATZ
Grant Thornton

JOHN KENNEDY
CenturyLink

AAMIR KHAN
CGI Federal

ANIRUDH KULKARNI
CVP Corporation

HA LE
Grant Thornton

KIMBERLY LEE
Grant Thornton

KATHY LENTZ
Federal Insights, LLC

JASON LINTHICUM
Cisco

CLIFF LOWRIE
Deloitte

DANIELLE MANSON
Brocade

DAVE MARTIN
Teradata Government Systems LLC

DAVE MCGINN
Hewlett-Packard

MICHAEL MCINTIRE
LMI

IAN MOORE
General Dynamics Information Technology

REBECC MOSS
Lockheed Martin

DEIRDRE MURRAY
CenturyLink

KYHATI NAYAK
Grant Thornton

EVAN PANAYI
Grant Thornton

TOSS PANTEZZI
ICF International

SHARON PAYNE
Verizon

JIM VANDE PUTTE
Grant Thornton

COLIN RODGERS
Grant Thornton

AMY RASMUSSEN
Engility Corp

LARRY REAGAN
Maximus

YAMINI SAHARI
TechBlue

BRADLEY SAULL
PSC

MATT SHANKLE
Grant Thornton

BRENT SHOEMAKER
Federal Insights, LLC

SUSAN SMOTER
HPE

TODD SNEDDEN
CACI

LORI STALLARD
Leidos

RAYMOND STRUBLE
CenturyLink

ROBERT STURM
CGI Federal

MARY SWANN
IBM

SEAN SPANN
Buchanan & Edwards

LORI STALLARD
Lockheed Martin

SIMON SZYKMAN
Attain

WEI TANG
Grant Thornton

KATHY TAYLOR
DRT Strategies

CYNDI THOMAS
NCI Inc.

KATE THOMAS
CGI Federal

RICHARD THIELEN
CenturyLink

AARTI TRIVEDI
Grant Thornton

SONJA TWIFORD
Grant Thornton

MONTARIOUS USHER
Grant Thornton

DAVID VENNERGRUND
SalientCRGT

MIKE VOGEL
Harris

EMILY WAI
Grant Thornton

BRAD WILHELM
Grant Thornton

ANTOINETTE WILLIAMS
Federal Insights, LLC

KATHRYN WOODWARD
General Dynamics

TOM WOTEKI
Maximus

ACKNOWLEDGMENTS

We thank federal CIOs and CISOs for participating in this year's survey. We also acknowledge the support and contributions of the sponsoring organizations and the time and expertise of the individuals listed in this report. To obtain copies of this report and the survey questionnaires, visit any of the websites listed below.

PROFESSIONAL SERVICES COUNCIL

4401 Wilson Blvd #1110
Arlington, VA 22203
(703) 875-8059
www.pscouncil.org
David M. Wennergren
Executive Vice President, Operations and Technology

The Professional Services Council (PSC) is the voice of the government technology and professional services industry. PSC is the most respected industry leader on legislative and regulatory issues related to government acquisition, business and technology. PSC helps shape public policy, leads strategic coalitions, and works to build consensus between government and industry. PSC's more than 400 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the trade association's members employ hundreds of thousands of Americans in all 50 states. Learn more about PSC at www.pscouncil.org.

GRANT THORNTON PUBLIC SECTOR

333 John Carlyle Street, Suite 400
Alexandria, VA 22314
703.837.4400
www.GrantThornton.com/publicsector
George DelPrete
Principal, Information Technology

Grant Thornton Public Sector helps executives and managers at all levels of government maximize their performance and efficiency in the face of ever tightening budgets and increased demand for services. We give clients creative, cost-effective solutions that enhance their acquisition, financial, human capital, information technology, and performance management. Our commitment to public sector success is burnished by a widely recognized body of thought leadership analyzing and recommending solutions to government's greatest challenges.

Based in the Washington D.C. metropolitan area, with offices in Alexandria, Virginia; Austin and San Antonio, Texas; Tallahassee, Florida, and Los Angeles and Sacramento, California; Grant Thornton Public Sector serves federal, state, local, and international governments. For more information, visit grantthornton.com/publicsector.


LIVE CHAT
-MEDIA
-PHOTOS
-VIDEOS
-MUSIC
RDW
TRG
RTG
WEF
HRT
-CULTURE
-ECONOMIC
-FINANCE
-BUSINESS
-EUROPE