2014 TechAmerica Federal CIO and CISO Survey

TechAmerica
Powered by CompTIA

Grant Thornton

CIO/CISO Insights

Achieving Results and Confronting Obstacles

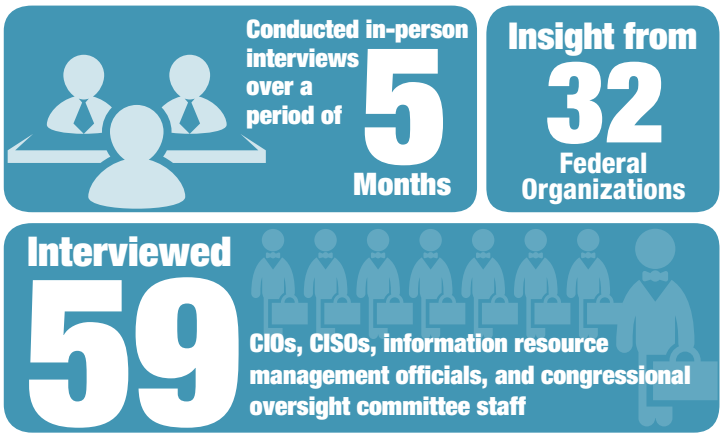
TABLE OF CONTENTS

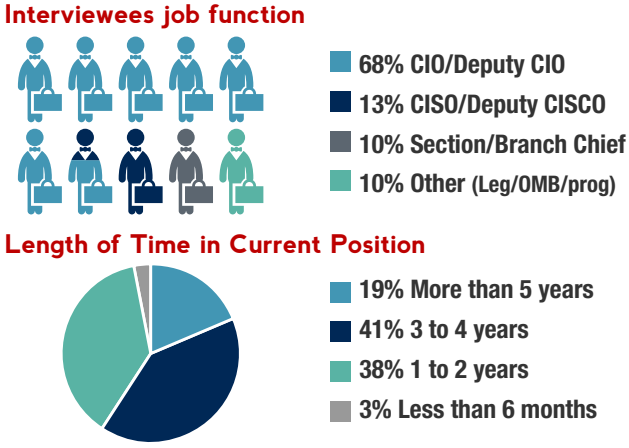
ABOUT THE SURVEY

PURPOSE AND METHODOLOGY

TechAmerica has surveyed Federal CIOs for 24 years, and this year we expanded to include CISOs. Through these surveys, top IT officials, oversight groups, and congressional staff shared their views on challenges facing Federal CIOs. As in past years, TechAmerica received outstanding support from the Federal CIO / CISO community and from Grant Thornton LLP, which sponsored and led this survey. However, to preserve anonymity, we do not attribute responses to specific individuals.

Readers may download copies of this and prior surveys at *http://www.techamerica.org/cio-survey/*





EXECUTIVE SUMMARY

TechAmerica has conducted an annual Federal government Chief Information Officer (CIO) survey for 24 years, with the support of Grant Thornton LLP. In 2014, 59 information technology (IT) leaders (see Appendix A) participated in the survey, including CIOs of major federal departments and staff from OMB and the Capitol Hill. Professionals from TechAmerica member firms conducted the interviews (see Appendix B).

The 24th report of Federal CIOs occurred in a year of many challenges. The CIO community endured the effects of a bitterly divided Congress that resulted in sequestration and a government shutdown, along with unprecedented leadership turnover of Federal CIOs and a major IT implementation failure, Healthcare.gov. It is against this backdrop that we sought insight from CIOs on how they are providing innovative technology solution to their customers. This dedicated cadre of technology professionals is working diligently to improve how government uses technology to deliver services to its constituents. Many Federal leaders are doing just that and coming up with creative ways to navigate through what seem to be perpetual challenges: security, funding, and workforce.

We organized this year's survey around an analysis of the top priorities and challenges facing CIOs followed by a series of questions related to the four priorities in the President's FY14 IT budget – innovating for the American people; delivering to improve the return on investment in Federal IT; protection to advance our nation's cyber security; and analyzing data to make business decisions that achieve results.

Top priorities for CIOs include: improving cyber security, modernizing/transforming IT operations, migrating to the cloud and maturing mobility. While there is much work to do in these areas, CIOs are making headway moving to continuous monitoring for cyber, using agile techniques to simplify IT modernization and "walking not running" toward cloud and mobile. Top challenges include workforce, cyber security and budget. While CIOs have a dedicated workforce, they still continually ace the need to navigate through the impacts of budget cuts on hiring, skills gaps and workload imbalances on performance. The internal and external cyber threats facing CIOs continue to grow. Finally, CIOs survived the shutdown, but still feel as if too much of the limited IT dollars go to fund operations and maintenance, and IT infrastructure, as opposed to development, modernization and enhancement.

INNOVATE FOR THE AMERICAN PEOPLE

Innovation across the Federal sector ranged from increased use of cloud and mobile services to identifying new ways to communicate and secure the IT infrastructure. Ninety percent of respondents stated that their organizations had moved to the cloud, in at least some capacity. Furthermore, CIOs are working feverishly to improve delivery of services through mobile devices, while managing workforce challenges relating to skill gaps, budget cuts and recruiting and retention.

DELIVER – IMPROVE THE RETURN ON INVESTMENT IN FEDERAL IT

Federal agencies continue to drive towards reducing redundancies and increasing efficiencies through efforts such as the move to shared services and the expanded focus of PortfolioStat. CIOs complained acquisition policies and practices that still hinder agencies' ability to take advantage of new technologies quickly.

PROTECT – ADVANCE OUR NATION'S CYBERSECURITY

Cybersecurity and the protection of Federal IT assets continues to be an important focus of Federal CIOs and CISOs. Most of the agencies with whom we spoke were able to use the Federal Risk and Authorization Management Program (FedRAMP) to reduce the risks of moving to cloud services. Furthermore, agencies are shifting toward continuous monitoring to move toward real time analysis and more effective sharing of best practices and lessons learned between agencies.

ANALYZE

Data has always been a major driver of decisions for Federal CIOs and CISOs. With the depth and breadth of data available growing each day, the management of data becomes key. We asked CIOs to rate themselves on their level of maturity with analytics, however, none rated themselves very effective; the majority said they were moderate to just getting started. They are working to improve information sharing, data quality, and improving the ability to derive valuable information from the "gold mine" of data they possess.

SECTION 1: FEDERAL IT OVERVIEW

Multiple factors, both internal and external to CIO shops, influence Federal IT priorities. We asked CIOs to identify their top three priorities and challenges. Here is what they said:

TOP 3 PRIORITIES			TOP 3 CHALLENGES		
#1	#2	#3	#1	#2	#3
CYBERSECURITY/IT SECURITY	MODERNIZATION/ INNOVATION	CLOUD/ MOBILITY	HUMAN CAPITAL/WORKFORCE	CYBERSECURITY/IT SECURITY	BUDGET/ COSTS/SAVINGS
Cybersecurity has remained at the forefront of CIOs' priorities as agencies move to continuous monitoring.	The majority of CIOs are moving to shared service providers, and/or cloud solutions. Many CIOs and CISOs also saw the replacement of legacy systems as a top priority for their offices.	The increased use of cloud services and or mobility is a key priority. For example, one respondent stated that "standing up web services, smart phone pilots, and bring your own device" were all high on his list.	Federal IT leaders indicated that workforce balancing, competency development, and attracting and retaining talent remains the top challenge.	As in previous years cybersecurity threats continue to be a top challenge across the federal government	Respondents stated that one of their top challenges included understanding costs and potential savings while fighting budget reductions
Other top priorities discussed included data management and analytics, open source, governance, infrastructure and operations, human capital, and consolidation/centralization of IT.			*Other top challenges discussed included culture, governance, data management analytics, acquisition, and benefits realization.*		

Once again this year cybersecurity was identified as a top priority and a top challenge for Federal CIOs. One respondent stated that over the next year, they want to "put in place IT controls from the beginning of the [development] process, allowing for greater innovation." Another stated the top priority will be to "transform the cybersecurity mindset from compliance to a risk management perspective," aligning to the continuous monitoring model, as well as the federal risk and authorization management program.

Modernization and innovation to replace out-of-date technology was identified as a top priority for those surveyed. Twenty percent specifically pointed to the increase use of cloud services and or mobility as key priority. Other top priorities discussed included data management and analytics, open source, governance, infrastructure and operations, human capital, and consolidation/centralization of IT.

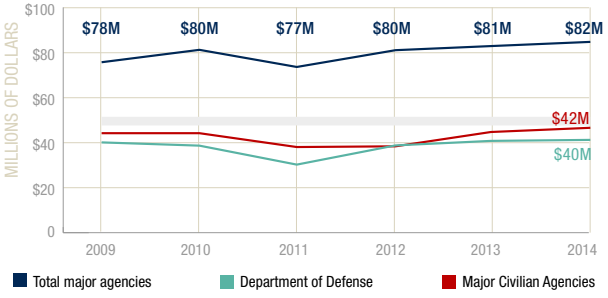
The top three challenges reflect many of the same concerns raised by CIOs last year. The top challenge perceived by CIOs and CISOs included human capital or workforce issues, where one respondent stated they were "five years behind in terms of talent." Fifty-two percent of respondents identified this as a top issue. Forty-five percent of IT leaders indicated that cybersecurity and IT Security continue to be a top challenge across the federal government. Approximately 11% of those with whom we spoke stated that one of their top challenges included understanding costs and potential savings.

HOW THE IT BUDGET IS BEING SPENT

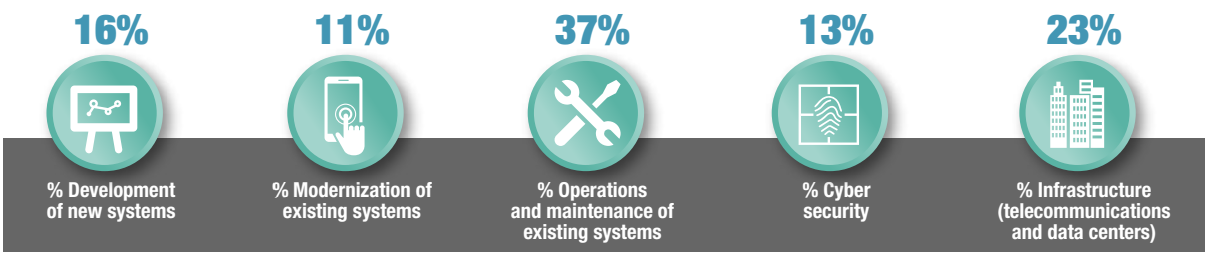
In 2014 we also saw a slight 2% increase in spending for major civilian agencies from $41.8M to $42.4M. Department of Defense also saw increase of $789K from $38.8M to $39.6M.

As in previous years, CIOs continue to spend most of their IT budgets on the operations and maintenance (O&M) of existing systems and infrastructure, although this year we did notice an interesting shift in funding. In 2013 we reported that agencies were spending approximately 85% on O&M, infrastructure, and cybersecurity. This year funds directed in these areas

Trend in federal IT spending over time



How are IT dollars spent?



dropped by over 10 percentage points to 73%, showing the shift in focus towards development and modernization (DME). OMB and GAO have often pointed to the imbalance of spending between O&M and DME. With the goal of shifting those funds toward new development and modernization, OMB has kicked off multiple initiatives attempting to reduce duplication and increase efficiencies, such as PortfolioStat. Within this fiscally constrained environment, Federal CIO shops are gradually turning the focus to developing with less resources, highlighting the need to implement innovative and cost-effective technology and processes.

CIO CONTROL

In recent years, GAO and others have focused on the CIO's control over agency funds. Last year survey respondents indicated that while the department CIO had the primary responsibility for IT spending, authority was also spread across component-level or bureau CIOs and program offices. Many CIOs felt this made it difficult for them to reduce enterprise IT spending. This year we asked CIOs to rank the percentage of budget they controlled. About half of the respondents indicated that CIOs control less than 50% of the budget. A quarter of that group indicated that they believe CIOs have less than 25% of control. Regardless, nearly all respondents indicated that over this past year they have had more insight into how IT dollars are being spent.

POINT

"The Agency needs to do a better job of centralizing IT under the OCIO and actually withholding the IT spending dollars from the operational programs, thus forcing the money to be properly spent under the OCIO umbrella"

COUNTER POINT

"OCIO should not dictate budgets completely; the mission should have the final say."

ARE LEGISLATIVE OR POLICY CHANGES NEEDED?

We asked CIOs and CISOs what, if any, legislative or policy changes they believed would assist their organization in becoming more efficient. Twenty-seven percent stated that legislation and policy were not needed. "You can't legislate good ideas and you can't legislate the roles needed to properly do the job." Another respondent stated that the focus should be on increasing transparency and the use of governance bodies such as the CIO Council. There were mixed reviews of the Federal IT Acquisition Reform Act (FITARA) Most CIOs were against the requirement in that bill that all CIOs would need to be politically appointed, and felt the congressionally mandated reporting would result in another unfunded mandate. On the other side, 15% of respondents indicated the legislative and policy changes related to centralization of IT under the CIO's control is necessary, one saying "anything that provides more control over IT spending decisions is helpful". One respondent stated that legislation, like the Federal Information Security Management Act of 2002 (FISMA), "fails to solve problems – it requires more reporting, but doesn't drive people to take action based on those reports. The result is the creation of a lot of information, which cost money to create." This respondent indicated that FISMA Reports are just a paper exercise.

The Federal IT Acquisition Reform Act (FITARA)

The current version of FITARA was passed by the House in April 2014, and calls for, among other things:

1. A modification to the designation/appointment of CIOs
2. The CIO Council to be designated as the lead interagency forum for coordination
3. Data center optimization
4. Changes to IT acquisition and the acquisition workforce

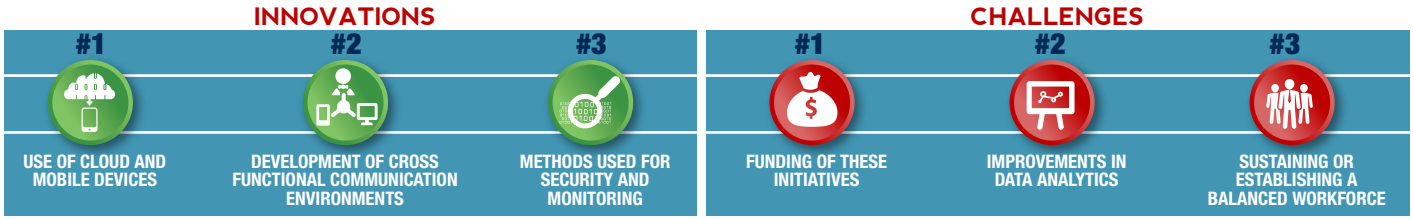
A Senate version of the bill is awaiting a vote.

"You can't legislate good ideas and you can't legislate the roles needed to properly do the job"

Of those that stated changes in legislation and/or policy change was needed, 18% suggested changes in Acquisition rules most notably reforming the Federal Acquisition Regulation (FAR). A number of other CIOs suggested a need for legislation to allow CIOs greater latitude for hiring on wages. Some respondents commented that the Clinger-Cohen Act gave effective legislative authority, however the government's execution has left the gap. Additional areas discussed by respondents include security legislation and overhauling the outdated FISMA legislation, and the changes needed to capital planning policy, such as OMB's Circular A-130.

SECTION 2: INNOVATE

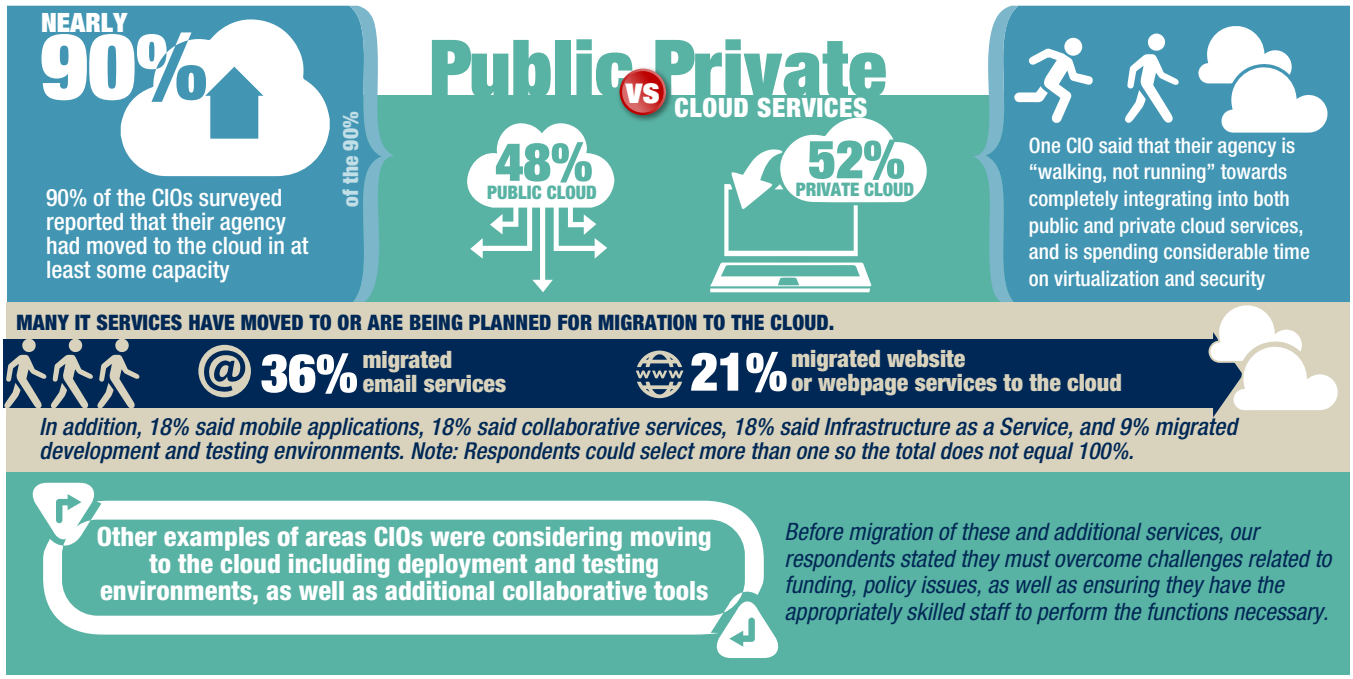
CIOs and CISOs are committed to adopting new technology to serve their constituents and to empower their workforce. The top three innovations identified include the use of Cloud and mobile devices; development of cross functional communication environments; and methods used for security and monitoring.



In addition to pursuing innovations in these areas, other respondents noted that governance and data management were key innovations. While these innovations have allowed agencies to grow and expand their IT services and management, multiple respondents identified the top challenges to innovation as funding of these initiatives; improvements in data analytics; and sustaining or establishing a balanced workforce.

CLOUD

The "Cloud First" policy required "each agency's CIO to fully migrate three services to a cloud solution by June 2012 and implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists".



Across our respondents, many IT services have moved to or are being planned for migration to the cloud. Of those who indicated that they had already moved services, 36% migrated email services. One agency said it expected to save more than $50m over 5 years by moving enterprise email to the cloud, while another stated, "Cloud hasn't delivered the savings promised." Our respondents also provided examples of areas they were considering moving to the cloud: deployment and testing environments, platform as a service, talent and performance management services, and collaborative tools.

CIOs are working to navigate through the following top cloud challenges: acquiring a knowledgeable workforce, ensuring interoperability, the cost of cloud licenses, security, and accessibility of data and information. CIOs are navigating a labyrinth of cloud challenges:

> "As new applications are being developed, they are actually developed in (our private cloud), and by using a standardized software development kit, applications can more quickly be put into production."

recruiting and retaining an adequately knowledgeable workforce, ensuring interoperability, managing the cost of cloud licenses, ensuring adequate security, and broadening accessibility of data. One respondent said that he not only "needed a robust workforce skillset including big data analysts, product managers and vendor managers, but he also needed client domains to be mature enough for cloud computing."

Rigorous cloud planning and developing an understanding of IT costing before migration are critical success factors in migration to cloud services. On a more granular level, as agencies consider moving to the cloud, CIO respondents stated that setting business goals and target outcomes is critical to successful implementation, as well. The primary challenge with the use of this technology is ensuring security requirements are properly and adequately covered: "You cannot decouple a move to the Cloud from your security strategy."

"Ensure that we have all requirements upfront. Having clear IT, legal, contractual, security, records, etc., requirements is important because often times, you have no recourse once you have signed with your providers. You must make sure you know who is taking on the accountability when moving to the cloud."

Data storage costs and contracts were also cited as major challenges. In some cases, respondents told us, government pays only for storage used. But in others, it pays for an allocation of storage whether or not it is fully utilized. The latter requires CIOs to pay a premium for data storage even when it's not needed, suggesting providers ought to consider different cost models. "I'm not buying a herd of cattle," on respondent said. "I'm buying a bottle of milk." It may be time to change the data storage business model.

MOBILITY

In the past few years, the use of mobile devices across the Federal government has shifted from a nice-to-have to a stakeholder requirement. The mobile device market and, to a lesser extent, applications, are driven by the end-user, forcing CIOs and CISOs to adopt fluid, constantly evolving governance structures that enable enterprise-wide value and ease-of-use, while wrapping organizational data in a robust security blanket. While it is difficult to hit a moving target, the Federal and commercial communities are collaborating on solutions. Derived credentials are at the forefront of mobile security discussions because they leverage the strength of Public Key Infrastructure (PKI) authentication and identity proofing, in which the Federal Government has already invested billions of dollars to meet Homeland Security Presidential Directive-12 (HSPD-12) requirements for Personal Identity Identification (PIV) Credentials. By securing the data transfer between mobile devices and a host, CIOs can take advantage of additional investment in Cloud Services and virtualization, leaving the physical devices free of agency data. As of this writing, the National Institute of Standards and Technology (NIST) is in the draft phase of Special Publication (SP) 800-157, Guidelines for Derived PIV Credentials and the market place offers a variety of working technologies that range from a PIV sled that attaches to mobile devices, to integrated circuit chips.

Killer government apps!

- Law Enforcement agents use a quick-capture fingerprint app to quickly ID suspected bad guys in the field
- Citizens can use an application to report and map marine debris to scientists for further analysis
- 24/7 virtual assistance and tips on preventing food-borne illness, safe food handling and storage, and preparation

Defining mobile governance often starts with device ownership – government furnished devices, offering greater control, versus Bring Your Own Device (BYOD). Our CIOs grasp the importance of allowing their stakeholders to use their own devices, but must deal with the security issues it presents. CIOs and CISOs can manage agency data, internal applications, and user behavior within their own network, but struggle with the realities of personal usage. Advances in Mobile Device Management (MDM) have resulted in the ability to create data partitions within a mobile device so that personal usage cannot infect agency data and the Federal Government does not have a window into a user's private affairs – this solution is widely considered by CIOs to be one of the few mutually beneficial security measures. Another reality of the BYOD is the increased likelihood of a device being lost or stolen. According to the Federal Communications Commission, cellphone theft accounts for 30-40% of robberies in United States cities: a statistic that frightens any CIO or CISO charged with managing mobile devices. In response, our Government's leaders have successfully called for wireless carriers to include a "kill switch" on all cellphones, allowing them to be immediately terminated if a phone goes missing. In April 2014, major carriers and manufacturers, including Apple, Google, Samsung, and Nokia, signed the "Smartphone Anti-Theft Voluntary Commitment," a non-binding pledge to include a Kill Switch on all phones manufactured after July 2015. One BYOD governance policy that leaves CIOs scratching their heads is how to manage devices that are no longer

supported by their carriers, which can occur as quickly as 24 months from the original purchase date. With the support of the vendor community and government-wide collaboration, programs like the General Services Administration's (GSA) Managed Mobility Program are driving these discussions and connecting CIOs and CISOs to MDM resources that help them create functional and realistic governance frameworks around these issues.

Biggest barriers to increase mobile use

We asked CIO's to identify the biggest barriers to the increased use of mobile in your organizations:

- Security
- Policy
- Governance
- Identity management
- Culture
- Effective business case and technology architecture

We asked CIOs to identify the biggest barriers to the increased use of mobile in their organizations. For Federal CIOs and CISOs to empower a connected, mobile workforce for the 21st Century, continuous collaboration is required. The mobile marketplace advances too rapidly, without regard to the needs of the Federal Government, for agencies to operate in isolation and, fortunately, many of the security, governance, and ROI challenges they face are similar enough for effective device and agency agnostic solutions. The government is starting down the right path with highly anticipated NIST guidance, the CIO Council's Mobile Computing Decision Framework to help agencies assess their readiness and risk levels, and with GSA's Managed Mobility Program, offering resources on MDM and MAM, as well as Mobile Lifecycle and Mobile Expense Management. These tools offer CIOs and CISOs a starting point for quickly and effectively leveraging mobile technology. We hope that as the mobile community expands these, governance tools continue to be updated and expanded at the same pace as the mobile marketplace.

FUTURE READY WORKFORCE

CIOs want to equip their workforce with the competencies and skills, modern tools, technologies, and policies to engage in fulfilling the agency's mission. During these tight budget times, the Federal government must be strategic in its use of technology and empower its workforce to provide internal and external stakeholders with needed services. Critical factors such as declining budgets, impacts of sequestration and shutdowns, and a workforce that is retirement eligible, and overworked are impacting the ability of CIOs to meet requirements and plan for the future. For the immediate future, CIOs must address a declining pool of contractors and Federal workers with the right skills and competencies, the impact of retirements, and a need for competencies including project management, leadership, business acumen, and strategic planning.

Current Challenges

CIOs identified several key challenges to completing their mission: the need for workforce planning; the impact of budget cuts on hiring, skills gaps, and workload imbalances on performance; the need to develop a workforce with a changing set of skills and competencies; and the ability to attract and retain the workforce of the future.

TOP CIO WORKFORCE CHALLENGES

In general, agencies stated they are not using all of the data available to them to support business-driven decision making. While some agencies are further along in using data analytics to support the development of realistic CIO budgets and resource plans, most are in the beginning stages of collecting and analyzing this information and integrating it into the planning and budget processes. CIOs are managing their cost data but they are struggling to understand their workload and skills data to plan for their future workforce. As noted by the survey participants, this continues to be a high priority.

> "Our greatest strength is our workforce and their dedication to the mission."

Recent budget cuts have taken their toll on the CIO's ability to manage the increasing needs of the organization. CIOs are struggling with reductions in people. Even when resources are available, there is a shortage of workers with the skills needed to manage new programs and technology. In many agencies, technology skills are housed in the contractor workforce. As contractor budgets are reduced, the Federal workforce is expected to take on more of the work formerly completed by contractors even though they often lack the skills to assume these responsibilities. A reduction in budget for training, conferences, and other programs such as internships and rotations exacerbate this gap.

Changes in the type of work, agency priorities, and emerging requirements are demanding a workforce with up-to-date

"We have a huge amount of institutional knowledge, but they are getting ready to retire. We don't know where the next generation of Federal employees will come from to fill the gap."

skills and competencies. CIOs report they need a workforce with competencies in data analytics, acquisition, customer service, business acumen, and program and project management, especially related to agile development. Formal training and certifications, on the job learning, and other types of developmental programs are needed or the skill gaps between the private sector and the Federal workforce will continue to grow.

Recruiting and Retention

Agencies continue to face challenges recruiting and retaining the best and brightest. One CIO stated, "We are using the same hiring processes we used over 50 years ago, and they don't work with the type of people we want to recruit." There is also a significant gap in engagement and satisfaction reported between entry level and journey-level workers. Coming up with a workplace that develops, nurtures, and engages workers at all levels continues to be a challenge for CIOs, especially in an environment where incentives and rewards for exceptional work are few and far between.

Succession planning continues to be a priority for CIOs because a significant amount of the Federal population is nearing retirement age. CIOs said that they do not have all the resources in-house to replace the retiring generation. Survey participants identified recruitment and retaining top talent as a challenge. They would like to see more IT innovation in government and bring "Silicon Valley to the Potomac".

Workforce balance

"As budgets continue to decline over the next four years, we expect to see additional reduction of the contractor workforce, as that is where it is easiest to make changes to address reduced budgets."

CIOs continue to try and find the "right" balance between Federal employees and contractors. Their goal is a core Federal workforce that can drive mission and manage programs with a contractor workforce that can be expanded and contracted to meet changes in requirements. However, current acquisition practices, budget cuts, the lack of project management skills in the Federal workforce, and rapidly changing technology make this one of their foremost challenges. While percentages vary, CIOs agree the goal is for the contractor workforce to supplement the Federal workforce in meeting surge requirements, bringing in specialized expertise, and helping to drive innovation. One thing is clear: simply shifting resources from contractor to Federal or vice versa is not the answer. Agencies should carefully plan any workforce balance shift to ensure that they are recruiting for the highest priority and mission critical skills gaps, while utilizing contractors for short term or surge requirements. The bottom line is that there needs to be a partnership between the two to ensure mission accomplishment, performance, and quality.

Competencies CIOs are looking for:

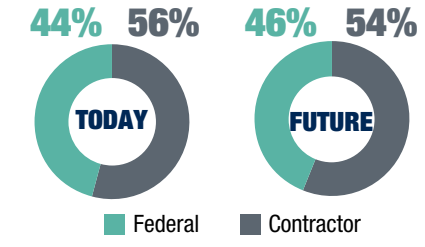
- Data analytics
- Acquisition
- Customer service
- Business acumen
- Program and project management (especially related to Agile)

Finally, government must address the recruitments process. Respondents expect to face the departure of 20-70% of their IT workforce in the next five years, and IT departments are not positioned to meet these challenges. The long waits for hires, the cumbersome processes, and the lack of modern technology only make the other challenges of filling vacancies and planning for turnover more difficult. Reform is necessary if CIOs are going to meet their goals. Agencies are maximizing the existing flexibilities within their human resource systems and policies. Additionally, agencies are using creative approaches to solve the challenges to attract and retain IT innovators. The dramatic growth in the cyber security workforce is driving one agency to try to change the legislative foundation for these requirements by pursuing a bill that would develop occupation classifications for individuals performing cyber activities, assess the readiness and capacity to meet the cybersecurity mission and allow other cyber-specific hiring authorities. CIOs acknowledge that these challenges are significant and continue to work towards short term solutions and long term strategies to position the organization for success.

Innovative ideas for addressing workforce challenges:

- Authority to direct hire-using options such as right-to-work model or front-end signing bonuses will help attract top talent.
- IT ROTC/reservist model, government pays for education in return for service rotations with industry
- Presidential Innovation Fellows
- Improved recruiting tools connected to social media, scholarships for service program through OPM, simplify ability to apply for government jobs– Monster needs overhaul
- Flexible work schedules and telework arrangements

Federal employee to contract ratio



SECTION 3: DELIVER

Modern IT development principles call for short incremental delivery of functionality, known as Agile development. While the adoption of Agile methods within industry emphasizes the early and continuous software delivery, according to GAO (GAO-12-681 and GAO-14-361), Federal agencies have had a mixed success moving towards and implementing OMB's guidance and incorporating the Agile principles. Eighty-three percent of respondents indicated their organizations are using Agile or rapid application development processes, but 40% reported their organizations lacked the maturity and organizational knowledge to fully exploit the benefits of Agile. As a result of the challenges in organizational maturity, respondents noted that there is a mixed use of agile and waterfall development models across their organizations. One respondent stated, "Culture is an issue and OMB requirements and acquisitions make it difficult to use agile development." Another stated, "There is a need to be realistic about what Agile can be used for" and we need to ensure we do not "set the bar too high." Another noted his organization wanted to use Agile but ran into challenges because "contract vehicles did not have that (Agile) language embedded."

83% using Agile or rapid application development

40% (of the 83%) lacked maturity to exploit the benefits of Agile

As organizations have adopted, or attempted to adopt, Agile, the most common lesson learned centered around the importance of organizational change management. Agencies face a number of internal challenges in getting their staff to move to an iterative development model. As respondents highlighted and GAO has reinforced (GAO-14-361), "Until OMB issues realistic and clear guidance and agencies address the weaknesses in their incremental development policies, it will be difficult to deliver project capability more rapidly."

> "Many people in this business are perfectionists; so unless an application or program was perfect, they would not want to deploy it into production. Getting beyond this mindset took somewhat of a carrot and stick approach."

Respondents stated...

46% Organization/culture change required to execute agile successfully

A few CIOs noted the speed of delivery resulting from Agile as a key improvement, which allowed "our customers [to have] an earlier look into the solution, with less rework." Some of the major lessons learned included the need for discipline and sophistication. One respondent stated, "we always do an assessment of the customer" up front to make sure they are ready before we begin," and "business and IT resources should merge into permanent cross-functional teams." Other problems cited included the extent of documentation. "The vendor went too far with regard to limiting documentation," one respondent said. "While that may work in industry, the Federal Government needs more documentation." Another respondent summarized the concerns with Agile by saying, "We need more focus on 'being done' instead of on internal IT speak. Ultimately, it doesn't matter until you're finished."

The respondents are looking for industry to drive government change and adoption by "coming up with frameworks as options, we haven't locked in on yet." By acknowledging the difficulty for the Federal workforce to stay current, respondents are looking towards industry to bring in experts that can engage with them and their employees, impart knowledge and leading practices, and set their organization on a path for success

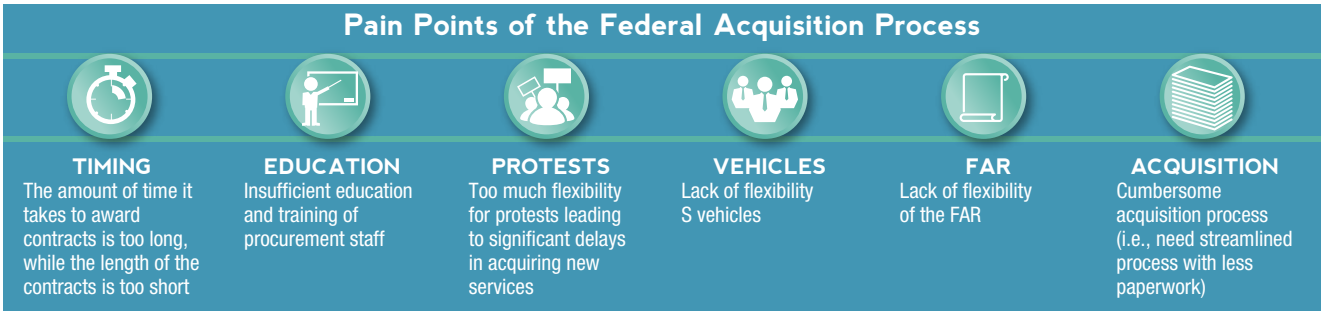
Top three ways industry can support government's use of Agile?

- Provide guidelines and processes for the effective use and implementation of Agile
- Provide education and training to government employees
- Provide clear examples of successful Agile projects

ACQUISITION

This year's Federal CIO survey highlights a number of challenges associated with procuring IT across the Federal government. Acquisition rules, people and processes have had a significant impact on the government's ability to deliver innovative IT in a timely manner. So the question remains, how can we minimize the frustrations of both

government agencies and industry so that we can successfully achieve innovation through efficient use of taxpayer dollars? We asked CIOs to identify the top things they would change with the procurement process. The responses included the following:



Should We Change the FAR?

CIOs expressed a number of thoughts about the Federal Acquisition Regulation (FAR). The majority suggested it should be overhauled, though a few suggested that the FAR serves its purpose. A summary of comments shared about the FAR follow.

So What Now?

Respondents expressed a common theme: we need faster ways to get new technology. One CIO elaborated, "The acquisition rules are not working. It takes six to nine months to get something in the door, but the technology has changed by then. We need to figure out how to get it faster." Another CIO at a large agency shared: "When I first took over this job, I worked with one guy from acquisitions who worked closely with us and understood our business and could produce contracts in 3 weeks compared to 4 to 5 months it takes others to produce. Today acquisition offices don't work as closely with us and they don't understand our business." While an overhaul or abandonment of the FAR rules in the near term is unlikely, there are steps the Federal government and industry can take to ease the burden and frustrations of the procurement process.

Ideas for solving IT acquisition challenges

- Pre-program Market Research
- More Oral Presentations
- Agencies share IDIQs for awarded BPAs
- Improved dialog between contracting officers, program staff and industry in planning stages
- Help contracting officers develop specialties in program areas and serve on details in programmatic roles

The FAR itself may not be the crux of our procurement pains, but rather, current Federal and industry practices and poor use of procurement tools hinders the delivery of innovative technology in a timely and effective manner. Aside from major legislative initiatives aimed at improving the Federal acquisition process, both the government and industry can make concerted efforts to be more proactive, transparent, and collaborative when it comes to identifying and preparing for IT needs sooner and responding with innovative IT solutions. Communication and collaboration between the government and industry needs to increase and begin sooner in order to foster a mutually beneficial relationship. Unfortunately, many agency procurement staff do not practice this.

Agencies can also take steps to alleviate common burdens experienced by working within the rules of the FAR to better attain innovative solutions. Agencies need to conduct "pre-program market research" before initiating the procurement process to understand what already exists in the market. Upfront research will help identify innovative solutions that have

"By the time a project goes through the whole process, the technology has changed...the solutions need to get to market faster."

SUMMARY STATISTICS FROM THE 2014 CIO SURVEY

Top areas where legislation could help

#1	#2	#3	#4
Acquisition	CIO Control	Workforce	Security

TOP 3 PRIORITIES

#1	#2	#3
CYBERSECURITY/IT SECURITY	MODERNIZATION/ INNOVATION	CLOUD/ MOBILITY
Cybersecurity has remained at the forefront of CIOs' priorities as agencies move to continuous monitoring.	The majority of CIOs are moving to shared service providers, and/or cloud solutions. Many CIOs and CISOs also saw the replacement of legacy systems as a top priority for their offices.	The increased use of cloud services and or mobility is a key priority. For example, one respondent stated that "standing up web services, smart phone pilots, and bring your own device' were all high on his list.

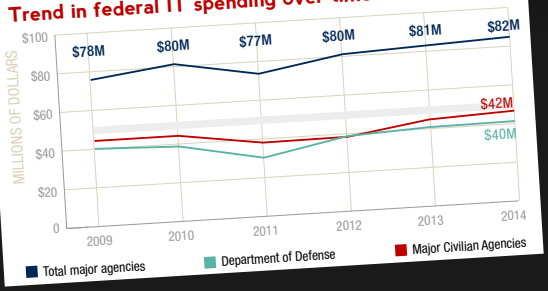
Other top priorities discussed included data management and analytics, open source, governance, infrastructure and operations, human capital, and consolidation/centralization of IT.

TOP 3 CHALLENGES

#1	#2	#3
HUMAN CAPITAL/WORKFORCE	CYBERSECURITY/IT SECURITY	BUDGET/ COSTS/SAVINGS
Federal IT leaders indicated that workforce balancing, competency development, and attracting and retaining talent remains the top challenge.	As in previous years cybersecurity threats continue to be a top challenge across the federal government	Respondents stated that one of their top challenges included understanding costs and potential savings while fighting budget reductions

Other top challenges discussed included culture, governance, data management analytics, acquisition, and benefits realization.

Trend in federal IT spending over time



How are IT dollars spent?

16%	11%	37%	13%	23%
% Development of new systems	% Modernization of existing systems	% Operations and maintenance of existing systems	% Cyber security	% Infrastructure (telecommunications and data centers)

The Federal IT Acquisition Reform Act (FITARA)

The current version of FITARA was passed by the House in April 2014, and calls for, among other things:

1. A modification to the designation/appointment of CIOs
2. The CIO Council to be designated as the lead interagency forum for coordination
3. Data center optimization
4. Changes to IT acquisition and the acquisition workforce

A Senate version of the bill is awaiting a vote.

INNOVATE

Killer government apps!

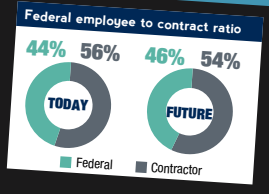
- Law Enforcement agents use a quick-capture fingerprint app to quickly ID suspected bad guys in the field
- Citizens can use an application to report and map marine debris to scientists for further analysis
- 24/7 virtual assistance and tips on preventing food-borne illness, safe food handling and storage, and preparation

Biggest barriers to increase mobile use

We asked CIO's to identify the biggest barriers to the increased use of mobile in your organizations:

- Security
- Policy
- Governance
- Identity management
- Culture
- Effective business case and technology architecture

Federal employee to contract ratio



INNOVATIONS

#1	#2	#3
USE OF CLOUD AND MOBILE DEVICES	DEVELOPMENT OF CROSS FUNCTIONAL COMMUNICATION ENVIRONMENTS	METHODS USED FOR SECURITY AND MONITORING

CHALLENGES

#1	#2	#3
FUNDING OF THESE INITIATIVES	IMPROVEMENTS IN DATA ANALYTICS	SUSTAINING OR ESTABLISHING A BALANCED WORKFORCE

TOP CIO WORKFORCE CHALLENGES

#1	#2	#3	#4	#5	#6
WORKFORCE PLANNING	BUDGET CUTS ON HIRING	SKILLS GAPS	WORKLOAD IMBALANCES ON PERFORMANCE	WORKFORCE CHANGING SKILLS/ COMPETENCIES	ATTRACT AND RETAIN THE WORKFORCE

Innovative ideas for addressing workforce challenges:

- Authority to direct hire-using options such as right-to-work model or front-end signing bonuses will help attract top talent.
- IT ROTC/reservist model, government pays for education in return for service rotations with industry
- Presidential Innovation Fellows
- Improved recruiting tools connected to social media, scholarships for service program through OPM, simplify ability to apply for government jobs– Monster needs overhaul
- Flexible work schedules and telework arrangements

Competencies CIOs are looking for:

- Data analytics
- Acquisition
- Customer service
- Business acumen
- Program and project management (especially related to Agile)

Public Private CLOUD SERVICES

NEARLY 90% of the 90%

90% of the CIOs surveyed reported that their agency had moved to the cloud in at least some capacity

48% PUBLIC CLOUD

52% PRIVATE CLOUD

One CIO said that their agency is "walking, not running" towards completely integrating into both public and private cloud services, and is spending considerable time on virtualization and security

MANY IT SERVICES HAVE MOVED TO OR ARE BEING PLANNED FOR MIGRATION TO THE CLOUD.

@ 36% migrated email services

21% migrated website or webpage services to the cloud

In addition, 18% said mobile applications, 18% said collaborative services, 18% said Infrastructure as a Service, and 9% migrated development and testing environments. Note: Respondents could select more than one so the total does not equal 100%.

Other examples of areas CIOs were considering moving to the cloud including deployment and testing environments, as well as additional collaborative tools

Before migration of these and additional services, our respondents stated they must overcome challenges related to funding, policy issues, as well as ensuring they have the appropriately skilled staff to perform the functions necessary.

DELIVER

Pain Points of the Federal Acquisition Process

TIMING
The amount of time it takes to award contracts is too long, while the length of the contracts is too short

EDUCATION
Insufficient education and training of procurement staff

PROTESTS
Too much flexibility for protests leading to significant delays in acquiring new services

VEHICLES
Lack of flexibility S vehicles

FAR
Lack of flexibility of the FAR

ACQUISITION
Cumbersome acquisition process (i.e., need streamlined process with less paperwork)

Ideas for solving IT acquisition challenges

- Pre-program Market Research
- More Oral Presentations
- Agencies share IDIQs for awarded BPAs
- Improved dialog between contracting officers, program staff and industry in planning stages
- Help contracting officers develop specialties in program areas and serve on details in programmatic roles

CHANGE THE FAR

"Abandon and rewrite the entire FAR…because the process is too long, even for small acquisitions, and with many holes."

"The FAR is not flexible; the rules don't allow for an acquisition process that incorporates the standards from industry."

"The FAR needs to be updated with fewer restrictions."

"The competitive environment is good, however, the acquisition process should be streamlined."

DO NOT CHANGE THE FAR

"The FAR should not be changed; the way in which the rules are used in practice should change."

"The rules are not the problem. The question is what can the procurement team do differently?"

"The organization needs to become a sophisticated buyer. Buying IT services is not like buying a hamburger; you're buying people, the unknown, and a promise. The acquisition team needs to use creativity to work within the rules."

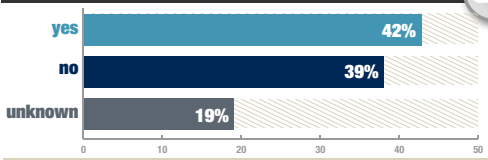
83% using Agile or rapid application development

40% lacked maturity to exploit the benefits of Agile (of the 83%)

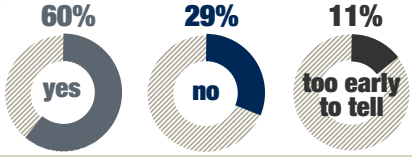
89% of CIOs and CISOs surveyed are currently using shared services

Common business functions that leverage shared services include financial services, acquisition, HR, payroll, travel, email, and other back-office functions

Has PortfolioStat Helped Reduce Redundant Spending?



Has PortfolioStat had an impact on your agency's understanding of IT spending?



Respondents stated...

46% Organization/culture change required to execute agile successfully

SHARED SERVICES: LESSONS LEARNED

- Business requirements must be clearly defined
- Cost-efficiency remains a focus
- Management and leadership remain flexible
- Ensure provider has capacity to meet needs
- Consider both industry and government solutions

Top three ways industry can support government's use of Agile?

- Provide guidelines and processes for the effective use and implementation of Agile
- Provide education and training to government employees
- Provide clear examples of successful Agile projects

PROTECT

WHAT CYBERSECURITY CHALLENGES DID RESPONDENTS HIGHLIGHT?

- Integrating security into the entire systems development life cycle so that issues are addressed upfront and during development, not merely after the fact
- Improving how security is integrated into operations
- Having the appropriate resources given transition from compliance to continuous monitoring
- Spending less time complying with regulations and completing assessments and devoting more energy to mitigating threats
- Having real time continuous diagnostics and mitigation tools to facilitate business decision-making

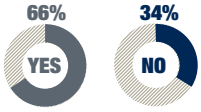
BEST PRACTICES

- Take a stem to stern look through networks for seams and cracks
- Identity enabled access controls
- Best practice sharing with other agencies
- Robust training program for workforce so they understand threats
- Thorough monitoring program
- Continuous monitoring
- Adoption of all NIST standards
- Neighborhood watch – talk in non-classified way about trends

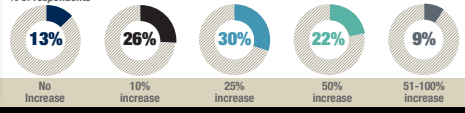
RECOMMENDATIONS TO IMPROVE FEDRAMP:

- Increase transparency
- Improve pricing and service offerings
- Increase the number of providers certified
- A more streamlined process allowing for quicker turnaround. One CIO suggested that the goal should be to get through FedRAMP process in 90 days.

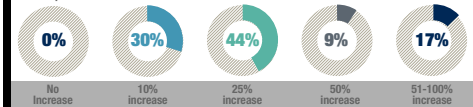
Respondents who have taken advantage of FEDRAMP for cloud service authorization



Eighty-seven percent of respondents indicated that their organizations have increased spending on cybersecurity



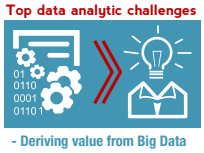
Increase of cyber threats over the last year



ANALYZE

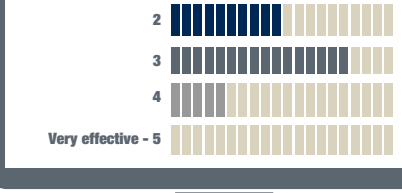
Organizations with Enterprise-wide Data Governance Strategies

Top data analytic challenges



- Deriving value from Big Data
- Poor data quality
- Lack of information sharing
- No "central vision"

Organizations' Level of Maturity Using Analytics



Data management and analysis challenges

BIG DATA
Challenge to derive value and meaningful information from massive amounts of data to ultimately inform decisions "They're sitting on a gold mine but don't know what they have yet..."

DATA QUALITY
Data management systems are plagued with severe data quality issues, which contribute to poor data integrity, reporting, and document management

INFORMATION SHARING
There is a lack of information sharing S and within government organizations

CENTRAL VISION
"We've been addressing challenges and needs in a haphazard manner, but with a central vision, we can be more consistent in our approaches so we get to what we want."

been developed and successfully deployed in the other government agencies. On the other hand, industry should seek an in-depth understanding of the Federal market landscape, contracting, acquisition strategy, and the procurement process through collaboration with and transparency from the government. Industry can leverage this understanding to share the latest technology innovations under development as potential, future solutions for the Federal government. Agencies can in turn be prepared to anticipate, solicit, and ultimately obtain these technologies faster before the "technology has already changed."

Lowest-Price Technically Acceptable (LPTA) Contracts

The government made an effort to ease some of the burdens of the acquisition process through the introduction of lowest-price technically acceptable (LPTA) contracts. LPTA contracts were primarily introduced as an effort to control costs, while also reducing the likelihood of protests and simplifying the procurement process by making requirements easier to fulfill. While LPTA contracts are an intended solution to procurement issues in a tighter fiscal environment, most believe LPTA contracts are not benefiting Federal agencies.

POSITIVE PERCEPTION:
"LPTA can be a valid tool for non-mission critical work, but it shouldn't be used for mission-critical work."

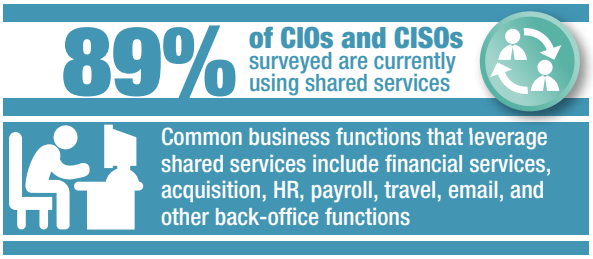
NEGATIVE PERCEPTION:
"I hate LPTA contracts. Surely, lowest price is a consideration, but not the deciding factor."

When asked about use of the LPTA contract type, several CIOs and CISOs indicated that they use and prefer Best-Value contracts. One CIO stated, "Contract folks tend to view success based on savings. As a result, you see a trend towards prices becoming the most important factor. I'm not sure that is the way to go." There is concern that LPTA contracts are forcing contractors to offer lower price solutions which can result in services that fall short of government expectations and are not as effective for the government in the long run.

One CIO stated, "We attempt to use this to stay within budgets, but we have to make sure that the results will still be achieved. You get what you pay for." LPTA is a trend CIOs don't like, and many feel it ultimately costs more money in the long run because LPTA contract winners have been stopped early due to performance issues, requiring the government to re-solicit. This ends up extending the program time lines and ultimate expenditure. CIOs believe LPTA contracts should be limited to commodities.

IT SHARED SERVICES

Of those we surveyed, 35% identified modernization and transformation as their top priority, many linking planned efforts to the move to shared service providers and/or cloud solutions. In a constrained budget environment, reducing waste and maximizing the return on investment for IT spending is the priority for many CIOs and CISOs. The majority of CIOs stated that they are currently using shared services.



CIOs and CISOs noted some important factors to consider before implementing shared services. One respondent noted that unique requirements are not well addressed by shared service providers, and it can be expensive to change from the status quo. When using shared services, business requirements become standardized across multiple agencies and/or organizations, and CIOs identified the need to adjust their expectations and foster a flexible environment. Further, respondents stated that shared service customers need to understand that they are losing a measure of control by using a shared service. In these cases, a lot of time and money will be spent rectifying problems when providers and customers cannot reach agreement. Respondents stated that in situations like this, clear communication, service level agreements, and leadership are essential for effective change management.

Multiple respondents stated that another significant lesson learned relates to challenges faced with agency budgets. CIOs need to make certain they have developed a comprehensive cost structure for shared services and that service providers have established accurate fee-setting models. Moreover, service providers and customers need to ensure that the cost of the service is being shared consistently with the use of the service. In an effort to manage budget challenges, it would be beneficial to leverage a shared services catalog whereby CIOs can reference existing shared services to better align current costs and performance before migration.

To facilitate growth, multiple CIO respondents stated that agencies can foster a more aggressive shared services design model, expand implementation government-wide rather than focusing within the agency, and push out shared services to end users. CIOs also cited shared services work best when they are not mandated but driven by a clear business case.

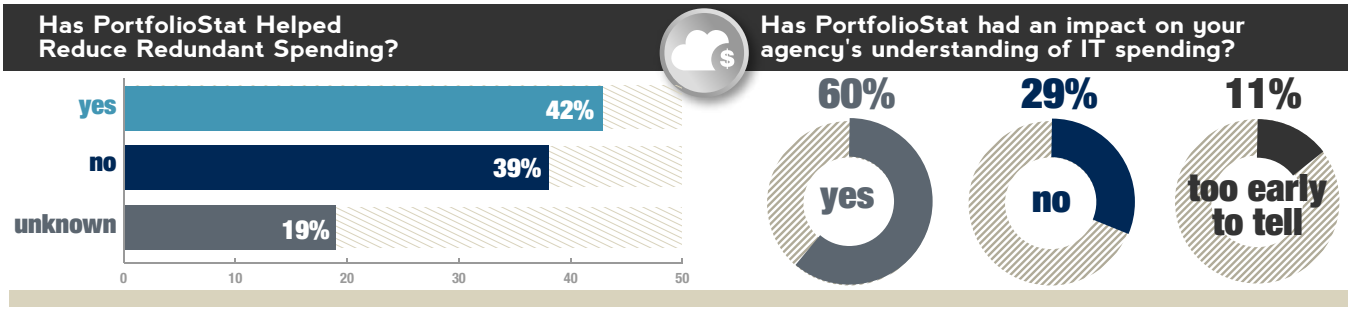
SHARED SERVICES: LESSONS LEARNED

- Business requirements must be clearly defined
- Cost-efficiency remains a focus
- Management and leadership remain flexible
- Ensure provider has capacity to meet needs
- Consider both industry and government solutions

As CIOs and CISOs continue to drive their agencies' goals and missions towards the reduction of duplication and inefficiencies, the use of shared services are not going away anytime soon. Reducing waste will continue to be a priority for agency leaders, and by leveraging past experiences CIOs will be able to better position themselves for successful future implementations. One CIO summarized the implementation and lessons learned of shared services best: "Know what you want to get out of the shared service and make sure your budget comparisons are accurate." Following this mindset can help progress the agency towards the goal of shared services, reducing redundancies and minimizing waste in the Federal IT space.

PORTFOLIOSTAT

While shared services is one way to reduce duplication and waste in the Federal IT space, another effort to maximize return on IT investments is through implementing PortfolioStat. PortfolioStat, the effort set forth by OMB in 2012, enables IT spending to be more transparent by reviewing an agency's portfolio management process. Mostly, it forced agencies to build a baseline and improve transparency into infrastructure investments.



As one participant noted, "It provides visibility into the need to reduce duplicative spending and the need to identify those instances of duplication." Eleven percent could not say whether or not it had an impact, because some indicated it is too early to tell any results since they just started the PortoflioStat last year. Others stated they did not have to participate in PortfolioStat.

Survey results also showed that agencies benefited from the process and saw a reduction in spending. Most respondents agreed that the intent of PortfolioStat is valuable, but some suggested the execution has had a minimal impact. CIOs received budget cuts and have been reviewing IT cost savings in duplication reduction and shared solutions. About 43% of respondents reported that PortfolioStat reduced redundant spending. It has improved the identification of cost avoidance and cost savings through the pressure that the tool places on decision makers. As with any new solution implementation, there are challenges to overcome. For example, some respondents do not believe PortfolioStat has had a major impact because although it provided a way to report the status of portfolios, many CIOs lack the authority to implement recommendations. Nineteen percent of respondents stated that they could not determine if PortfolioStat had helped reduce redundant spending. One respondent stated "spending and inventory data was not a very useful [metric] because of difficulties in making comparisons to other agencies." Additionally, these respondents stated that there should be more focus on segment architectures to ensure comparisons can be made.

SECTION 4: PROTECT

According to DHS, "Cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy." GAO notes, "Twenty-two of 24 major agencies identified information security as a major management challenge for their agency." Over the past 6 years, the number of incidents reported by Federal agencies to the Federal information security incident center has increased by nearly 680%. These incidents include unauthorized access to systems; improper use of computing resources; and the installation of malicious software. Consistent with these statistics, cybersecurity remains a prominent concern for CIOs. Two-thirds of respondents indicated that threats to their organization increased in the last year by at least 10%. Sixty-three percent of respondents identified cyber security issues as one of their top three priorities, which is more than twice as much as any other priority mentioned. CIOs highlighted a number of specific cyber security challenges.

> **"So many of the threats come in through individuals clicking on the wrong link or doing something that they just don't realize carries risks. User education is a big deal, phishing attacks, going to websites they shouldn't go to, building up networks, putting in the protection, it is constant risk management."**

WHAT CYBERSECURITY CHALLENGES DID RESPONDENTS HIGHLIGHT?

- Integrating security into the entire systems development life cycle so that issues are addressed upfront and during development, not merely after the fact
- Improving how security is integrated into operations
- Having the appropriate resources given transition from compliance to continuous monitoring
- Spending less time complying with regulations and completing assessments and devoting more energy to mitigating threats
- Having real time continuous diagnostics and mitigation tools to facilitate business decision-making

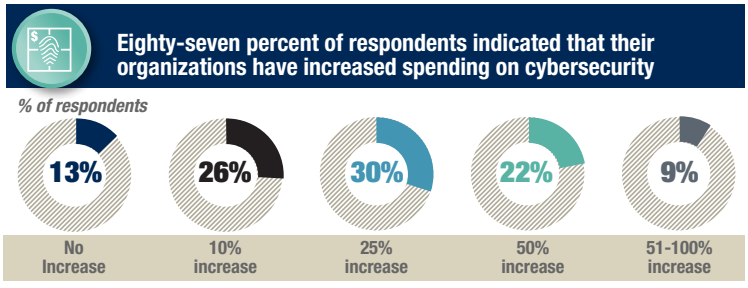
Effectiveness of your cyber program

When asked how CIOs measure effectiveness of cyber programs, CIOs responded with:

- The use of metrics, such as the number of incidents blocked, number of systems that are C&A certified, criticality, and report on performance (i.e., patching success, PII incidents)
- Executive dashboard (tracking training, POAMs, phishing attempts)
- Penetration testing
- FISMA Audits
- Self-assessments (including reviews by contractors and OIG)
- Analyzing real-time data on assets and vulnerabilities

Cyber spending

Current budgets allocate approximately 15% of IT funds to cyber security. The FY 15 budget requests $13 Billion to improve cyber security and expand continuous diagnostic technologies to mitigate threats nationwide. CIOs are supportive of the growth in cyber spending, but feel an increase will be needed in the coming years.



CONTINUOUS MONITORING

Continuous monitoring is a risk management approach to cyber security that maintains an accurate picture of an agency's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies. Survey respondents supported

continuous monitoring and feel implementation will help them mitigate cyber risks. CIOs provided the following insights on continuous monitoring and its benefits:

- Leveraging programs such as the DHS Continuous Monitoring as a Service (CMaaS) contract vehicle, to implement a continuous monitoring program to discover unauthorized or unmanaged hardware and applications, to identify inadequate or missing patches on networks and systems, and to ensure that baseline configuration settings are in place
- Shifting from traditional ways to manage security to real-time analysis
- Investing in tools that support the entire NIST Risk Management Framework (RMF) including loading documents, aggregating feeds, and performing assessments
- Participating in industry and government standards organizations and programs such as the Object Management Group (OMG) and the National Information Exchange Model (NIEM)
- Leveraging Federally Funded Research and Development Centers (FFRDCs) and Defense Advanced Research Projects Agency (DARPA) for research and development of continuous monitoring capabilities, tools and standards
- Focusing a portion of resources towards generic security practices while concentrating others on emerging and advanced threats
- Sharing best practices and lessons learned between agencies through governance groups such as the Federal CIO Council

BEST PRACTICES

- Take a stem to stern look through networks for seams and cracks
- Identity enabled access controls
- Best practice sharing with other agencies
- Robust training program for workforce so they understand threats
- Thorough monitoring program
- Continuous monitoring
- Adoption of all NIST standards
- Neighborhood watch – talk in non-classified way about trends

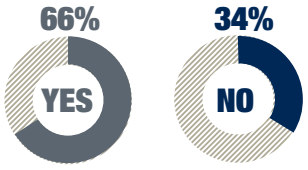
"Continuous monitoring is great. However, the NIST standards go back to an audit mindset. The question should not be if you are meeting the audit framework, it should be whether or not your information is protected. The NIST standard is not practical and not really relevant in the real world, it's too academic."

CIOs cited that the transition to continuous monitoring could create a big data problem. Federal agencies are dependent on sophisticated tools to capture data and logs being collected from network devices. The key will be to sift through this data and present actionable information to the right people at the right time. Agencies continue to integrate continuous monitoring into their other security processes including asset management, configuration management, and vulnerability management. Automation facilitates a full accounting of an agency's IT assets to identify and remove unmanaged assets so that those assets are under configuration management. Continuous Monitoring has also facilitated agency improvements in remediating against non-compliant baseline configurations and scanning assets for common vulnerabilities (software flaws, required patches, etc.). While CIOs acknowledge they have a long way to go to implement CM, most are optimistic about the improvements it will have on their cyber programs.

FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)

FedRAMPs standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services has been a key element to successful implementation of cloud computing. FedRAMP provides agencies a standardized set of processes, procedures, and controls to identify and assess risks and develop strategies to mitigate them. The majority of CIOs are using FedRAMP today. They had some ideas on how to improve FedRAMP.

Respondents who have taken advantage of FEDRAMP for cloud service authorization



Collaboration and partnership across the Federal government, with state, local, and tribal governments, internationally, and with the private sector will continue to be the key to securing the nation. As attacks become more sophisticated and technology advances, all organizations impacted must find ways to improve information sharing regarding threat remediation tactics, trends, and lessons learned. Organizations require common solutions that take less time to implement and that are flexible and scalable.

RECOMMENDATIONS TO IMPROVE FEDRAMP:

- Increase transparency
- Improve pricing and service offerings
- Increase the number of providers certified
- A more streamlined process allowing for quicker turnaround. One CIO suggested that the goal should be to get through FedRAMP process in 90 days.

All partners must continue to evolve the security and privacy controls they implement especially to maintain information security as new and innovative technologies are utilized to improve information access and service delivery.

SECTION 5: ANALYZE

With the abundance of data available to make decisions, CIO and CISOs have a real challenge of ensuring that there is a firm understanding of what data is useful and how it could be used to make evidence-based decisions. Open data policy has led to data management and analysis being moved to the forefront of CIO's priorities and initiatives.

Data management and analysis challenges

BIG DATA
Challenge to derive value and meaningful information from massive amounts of data to ultimately inform decisions "They're sitting on a gold mine but don't know what they have yet..."

DATA QUALITY
Data management systems are plagued with severe data quality issues, which contribute to poor data integrity, reporting, and document management

INFORMATION SHARING
There is a lack of information sharing S and within government organizations

CENTRAL VISION
"We've been addressing challenges and needs in a haphazard manner, but with a central vision, we can be more consistent in our approaches so we get to what we want."

With the proliferation of data generated in today's enterprises, data can be both a unique asset and a liability to CIOs. Properly managed and governed, data can be leveraged to effectively drive business strategies, gain operational efficiencies, and improve an organization's mission effectiveness. If it is improperly managed, it can provide misinformation, proliferate confusion, and be the source of enormous expenses to store and administer. Data management is a top priority mentioned by many CIOs this year.

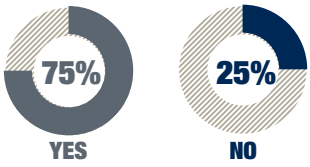
According to our respondents, the process of a) effectively converting raw data into useful and actionable information is obstructed by poor data quality, persistent data silos, and disparate visions and b) how to derive value from Big Data is one of the greatest challenges facing Federal CIOs.

Top data analytic challenges

- Deriving value from Big Data
- Poor data quality
- Lack of information sharing
- No "central vision"

We asked respondents to "rate your level of maturity using analytics across your organization." None of our respondents were able to state that they were "very effective" in their use of analytics and over 80% of respondents indicated that they were somewhere between "just getting started" and half way to reaching efficiency.

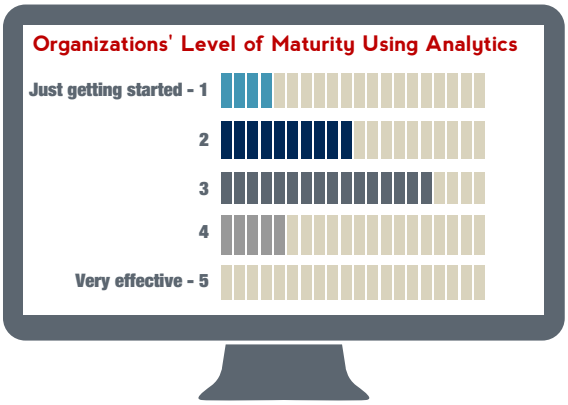
Organizations with Enterprise-wide Data Governance Strategies



When asked whether they had an enterprise-wide data governance strategy, 75% of respondents indicated that they do. The level of maturity of those strategies, however, had a wide range from having a "partial data reference model" to having a "robust" strategy. One CIO elaborated that his organization had "an overall governance strategy" that had independent components specific to the data warehouse, data integration, among others.

SOLUTIONS TO EFFECTIVE DATA MANAGEMENT AND USE OF ANALYTICS

The CIOs and CISOs interviewed touched on current initiatives or potential future solutions that are being considered to improve data management and use of analytics in their organizations. As shown, many agencies are still maturing in their use of analytics and data management.



CONCLUSION

FY 2014 has been one of both challenges and accomplishments for Federal IT leaders. As we move toward the end of fiscal year 2014, CIO's should reflect on many accomplishments of the past year and the strides toward building a better Federal IT Environment. Many CIOs overcame unprecedented budget constraints, sequestration and a government shutdown, and the criticism of Federal IT stewards during the failure of healthcare.gov to improve IT service delivery and lower costs through the use of shared services and enterprise-wide approaches to contracting, designing and building technologies. They also strengthened cyber programs through FedRamp and Continuous Monitoring, moved largely to agile development, and more effectively integrated mobile devices into their networks. These accomplishments and others have set the tone to position CIO's for future success.

As CIO's look ahead, they are cognizant that much work remains. First, they need to examine the unprecedented exodus of CIO's that occurred this year to understand why this occurred, what it means for the Federal IT community and craft a plan to mitigate a future drain of top talent and rebuild the pipeline of future CIO's. This is a key role that the CIO Council and OMB can play to ensure succession to the next generation of IT leaders.

CIO's also need to continue to improve delivery of Federal IT to take us into an era where citizens and federal employees can seamlessly and securely use mobile devices to do their jobs. While advances have occurred, failures like healthcare.gov and CIO's own acknowledgement that they aren't mature enough to achieve the benefits of agile, point to a need for continued improvement in how they develop and implement major IT programs. They also need to lead their enterprises to improve data analytic capabilities.

Unfortunately, CIO's have a long road ahead to solve their workforce challenges. They need new ways of understanding the skills they have and the workload of their staff. They also need to improve how they recruit and retain staff and provide education and training to teach staff the skills they need. CIO's desperately need to develop the next generation of IT leaders to create a succession plan for CIO's and IT leaders of the future. OPM has a significant role in this process and must provide CIO's and all federal executives with better tools and processes to recruit and reward great staff.

What CIO's buy will continue to change forcing modifications in how they buy? CIO's and the acquisition community need to collaborate to solve the perpetual acquisition challenges they experience. These issues will continue unless CIO's and their acquisition leaders learn to speak a common language and collaborate together, and with industry. OMB and the Hill should also explore ways to allow agencies to buy services off of other agencies IDIQ contracts to reduce the churn of acquisition many agencies go through in creating contracts for services which exist in other agencies.

Finally, while continuous monitoring is helping shine a brighter light on agency cyber issues, this is a journey that has just begun. There is much to learn, and CIO's must continue to innovate and improve information sharing to stay a step ahead of bad actors. The Government needs to use identity management and smart access controls to improve and regulate access to information. Additional resources and growth in cyber spending will be key to achieving this goal.

CIO's look forward to the new year and are confident they can continue to improve how they provide secure, cost effective IT services to their constituents. Whether developing new mobile applications to support agency missions, or by using data analytics to make informed, evidence-based decisions, CIOs are setting themselves up to be strategically positioned for success in the year ahead and are up to the challenge.

> **"Everything is evolving: video, mobile, I hear terms like 'big data,' but here's the problem: it's all new cars in old highways. Everyone is worrying about building cars but they're not worrying about building roads. You might have a nice car, but if you're driving home on I-66 in rush hour, good luck – because you're not going anywhere (no matter how nice your car is). Similarly, the IT infrastructure needs to be built up to be able to support constantly-evolving IT devices."**

APPENDIX A – LIST OF CIOS AND CISOS INTERVIEWED

Note: The titles and position of the government officials listed below were current at the time they were interviewed

DAVID ALEXANDER
Director
Geospatial Management Office Department of Homeland Security

DORINE ANDREWS
CIO
Peace Corps

CHARLIE ARMSTRONG
CIO
Customs and Border Protection
Department of Homeland Security

DARREN ASH
CIO
Nuclear Regulatory Commission
Department of Energy

FRANK BAITMAN
CIO
Deputy Assistant Secretary for Information Technology
Department for Health and Human Services

KEN BERMAN
CIO
International Trade Administration
Commerce

RICHARD BEUTEL
Senior Council
House Committee on Oversight and Gov't Reform
Congress

HORACE BLACKMAN
Director of VACO IT Support Service and
VA Central Office VACOCIO
Department of Veterans Affairs

SHANNON BROWN
CIO
U.S. Marshals Service
Department of Justice

JACQUIE BUTLER
CIO Staff
Agriculture Food and Nutrition Service

ROBERT CAREY
DOD Principal Deputy CIO
Department of Defense

KEVIN CHAREST
CISO
Office of the Assistant Secretary for Administration
Department for Health and Human Services

CHRIS CHILBERT
Chief Architect
Department of Homeland Security

PHILIP CLARK
CIO
Corporation for National and Community Service

CHERYL COOK
CIO
Department of Agriculture

KEVIN COOKE
Acting CIO
Department Housing and Urban Development

EMERY CSULAK
Deputy CISO
Department of Homeland Security

MARK DAY
Director of Strategic Programs
Federal Acquisition Service
General Services Administration

TOM DEBIASE
Deputy CIO
Immigration and Customs Enforcement
Department of Homeland Security

ELIZABETH DELNEGRO
CIO
Federal Acquisition Service
General Services Administration

DEBORAH DIAZ
Deputy CIO
National Aeronautics and Space Administration

JAMES FLANAGAN
Deputy CIO
Nuclear Regulatory Commission

PETER FONASH
CTO, Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

ROB FOSTER
Deputy CIO
Department of Health and Human Services

DEAN HALL
Deputy CIO and Associate Executive Assistant Director for IT Branch
Federal Bureau of Investigation
Department of Justice

JILL HARPER
Associate Director
Science and Management
National Institutes of Health

JOYCE HUNTER
Deputy CIO (Policy & Plng)
Department of Agriculture

CARLENE ILETO
Executive Director
Enterprise Business Management Office
Department of Homeland Security

JOSEPH KLIMAVICZ
CIO
National Oceanic and Atmospheric Administration
Commerce

MIKE KLOPP
Section Chief, IT Enterprise Management Section
Federal Bureau of Investigation
Department of Justice

JONATHAN KRADEN
Counsel and Senior Policy Analyst
Committee on Homeland Security and Govt Affairs
U.S. Senate
Congress

MICHAEL KRIEGER
Deputy CIO/G-6
Army
Department of Defense

WILLIAM LAY
Deputy CISO for Information Assurance
Bureau of Information Resource Management
Department of State

PHIL LETOWT
CTO
Immigration and Customs Enforcement
Department of Homeland Security

STANLEY LOWE
Deputy Assistant Secretary for Information Security
Office of Information Security
Department of Veterans Affairs

JAY MAHANAND
Deputy CIO
US Agency for International Development

NICOLE MATTISON
OI&T
Department of Veterans Affairs

CHARLES MCCLAM
Deputy CIO (Ops & Mgmt)
Department of Agriculture

JOHN MCGOWAN
Deputy Director for Science Mgmt & Operations
NIH/NIAID/OD/OSMO
Department of Health and Human Services

JON MCKEEBY
CIO
NIH, Clinical Center
Department of Health and Human Services

RICHARD MCKINNEY
CIO
Department of Transportation

KEVIN NALLY
CIO, Director C4
Marine Corps
Department of Defense

BRADLEY NIX
Director/CISO
Food and Nutrition Service
Department of Agriculture

THOMAS RICH
CISO
Nuclear Regulatory Commission
Department of Energy

SUSANNAH SCHILLER
CIO
Office of Information Systems Management, National Institute of Standards and Technology
Commerce

LISA SCHLOSSER
Deputy Administrator
Office of E-Government and Information Technology
Office of Management and Budget

RORY SCHULTZ
CIO
Food and Nutrition Service
Department of Agriculture

CHAD SHERIDAN
CIO
Risk Management Agency
Department of Agriculture

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

LARRY SWEET
CIO
National Aeronautics and Space Administration

SIMON SZYKMAN
CIO
Commerce

MIKE TARTAKOVSKY
CIO
NIH, National Institute of Allergy and Infectious Diseases
Department of Health and Human Services

MARY THOMAS
CIO
Department of Agriculture

KEITH TRIPPIE
Executive Director
Enterprise Systems Development Office
Department of Homeland Security

STEPHEN WARREN
Principal Deputy Assistant Secretary Office of Information and Technology Department of Veterans Affairs

BARRY WEST
CIO
Pension Benefit Guaranty Corporation

JERRY WILLIAMS
CIO
Office of Federal Student Aid
Department of Education

LARRY ZELVIN
Director
National Cybersecurity and Communications Integration Center National Protection and Program Directorate
DHS

BILL ZIELINSKI
Acting CIO
Social Security Administration

APPENDIX B – LIST OF INTERVIEWERS

Note: The organizations and companies of those listed below were current at the time the interviews were conducted.

TechAmerica Staff
MATTHEW KAZMIERCZAK

Grant Thornton Survey Team
GEORGE DELPRETE
THAD JUSZCZAK
CYNTHIA SWEERS
SAIRAH IJAZ
GLORIA FUNES

CIO Survey Interviewers
CRAIG ABELMAN
SAIC

TAMARA ANGER
Grant Thornton

KAKALI BANARJEE
SRA International

THELMA BARKER
CenturyLink

CAL BASSFORD
Grant Thornton

AARON BEASON
Grant Thornton

BOB BECK
NTT Data

CARRIE BOYLE
Grant thornton

TYRRELL BRAND
TIBCO

MICHAEL BRUCE
BAE Systems

VERN BUTLER
Grant Thornton

TONY CELESTE
Brocade

NILESH CHUDASAMA
Grant Thornton

LINDA CLARK
Robbins-Gioia

TOM COCOZZA
Grant Thornton

MARY COLLINS
SAIC

LAURIE COOK
SAS

THOMAS CRAVER
EMC2

DOUGLAS CRISCITELLO
Grant Thornton

JENSON DANIEL
Organon Advisors

ANAND M. DAS
Xerox Federal

BINTA DIATTA
Grant Thornton

KELLY DICKENS
CenturyLink

GIOVANNINA DIPIETRO
GDIT

DEBBIE DOWLING
Deep Water Point

ED DUBOIS
NetApp

SHAUN EDENS
TechFlow

DOUG GAINES
immixgroup, Inc.

GREG GARDNER
NetApp

MARTIN GILLESPIE
Salient Federal Solutions

MARK GIVENS
Grant Thornton

NANCY GRANDPRE
Century Link

ANTHONY GRAY
Salient Federal Solutions

CHRISTOPHER HEALY
Capgemini Government Solutions

DAVID HEMMER
Century Link

MARK HILBURGER
RedHat

JIM HILES
ASI Government

CHRISTIAN HOEHNER
Van Scoyoc Associates

THERESA HOLDER
Lockheed Martin

MARC HOLLANDER
Xerox

ANTONIS IOANNIDIS
SAIC

ROB IRISH
Grant Thornton

VIPIN JAIN
Hewlett Packard

CHARLES JAMES
Hewlett Packard

MIKE JELEPIS
SAS

CHAD JONES
Accenture

FELIZA KEPLER
Data Networks Corporation

DAVID KING
SAIC

BETHANY LEE
Grant Thornton

H. GIOVANNI LEUSCH-CARNAROLI
Grant Thornton

MARK LEWIS
Amazon Web Services

KRISTEN LILLARD
Grant Thornton

JASON LINTHICUM
CISCO

SHEILA LOWERY
OST, Inc

CLIFFORD LOWRIE
CACI – CMS Information Systems, Inc

LIZ LYDON
IT Cadre

ZAKIR MAHMOOD
Grant Thornton

EARL MADISON III
Lockheed Martin Corp.

BRAD MARCHAND
Grant Thornton

DAVID MARTIN
Teradata

TIMOTHY MAY
Salient Federal Solutions

DAVID MCGINN
Hewlett Packard

PAUL MEANEY
AT&T Government Solutions,

RICK MILLER
Red Hat, Inc.

KATHY MINCHEW
Federal Insights, LLC

DEIRDRE MURRAY
Century Link

ROB NESS
Grant Thornton

KEN NEWCOMER
ICF International

JIMMY NORRIS
Grant Thornton

JIM O'NEILL
Red Hat, Inc.

TODD PANTEZZI
ICF Intl.

NICK PAVSKI
Grant Thornton

DAVE PEARL
Grant Thornton

ANNE PETERA
Harris

TONYA POWERS
Accenture

CHAD RHEINGANS
Grant Thornton

RONALD RHODES
OST Inc.

GERRY ROBBINS
NJVC LLC

BRIAN ROSS
Harris Corporation

MIKKI ROSS
NetApp

ROLAND SCOTT
SRA

SURESH SHENOY
Information Management Consultants

BRENT SHOEMAKER
Level 3

BRIAN SKOLETSKY
Level 3 Communications

BETH SMITH
Deloitte

MARY SOUTHER
ASI Government

LORI STALLARD
General Dynamics

ROBERT STRICH
Century link

RAYMOND STRUBLE
CenturyLink Federal

MARY SULLIVAN
PwC

GREG SWANSON
Brocade

KENNETH TOULOUMES
Touloumes Group

OLIVIA TRIVISANI
CSC

IBRAHIM TUBBAJI
Verizon Enterprise Services

ROBERT TURNER
Xerox

RAMANI VAIDYANATHAN
SAP

STEVE VETTER
Hewlett Packard

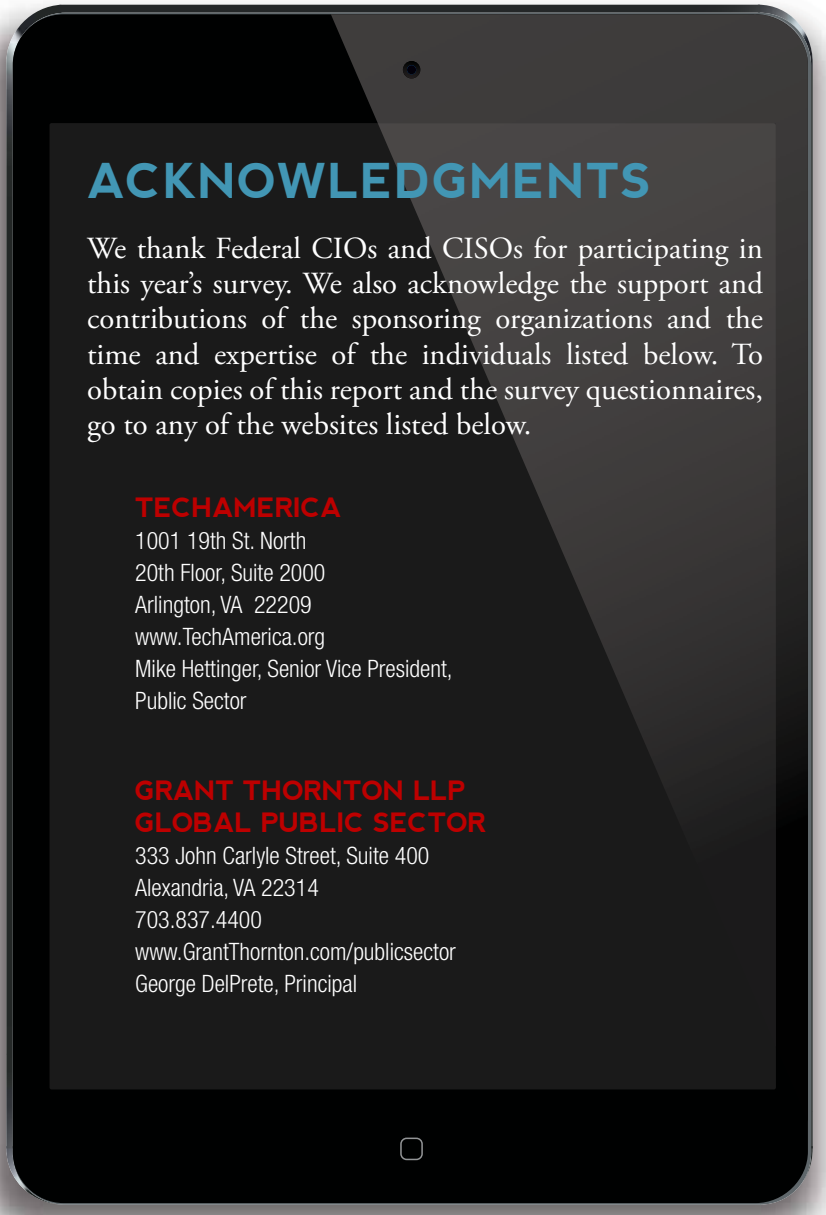
THOMAS J. VERVECK
Cybersalus

MARY WALL
Lockheed Martin

KATHRYN WOODWARD
General Dynamics

MATT ZIRPOLI
Harris IT Services

We would also like to acknowledge the following Grant Thornton staff in their support of the CIO survey:
Kim Adams, Bret Brikholz, Nina Dang, Justin George, Stephanie George, Virginia Gibson, Lisa Gryncewicz, Rebecca Lee, Tim Kenyon, John Konczyk, Moshe Nelson, Shannon Smith, Rhett Summers, Wei Tang, Eli Tucker, Derrick Turner



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 below. To obtain copies of this report and the survey questionnaires, go to any of the websites listed below.

TECHAMERICA
1001 19th St. North
20th Floor, Suite 2000
Arlington, VA 22209
www.TechAmerica.org
Mike Hettinger, Senior Vice President,
Public Sector

GRANT THORNTON LLP
GLOBAL PUBLIC SECTOR
333 John Carlyle Street, Suite 400
Alexandria, VA 22314
703.837.4400
www.GrantThornton.com/publicsector
George DelPrete, Principal

ABOUT THE SPONSORS

TECHAMERICA

TechAmerica is the public sector and public policy division of CompTIA, advocating before decision-makers at the state, Federal and international levels of government. Representing technology companies of all sizes, TechAmerica is committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world. With offices on Capitol Hill and in Northern Virginia, Silicon Valley and Europe, as well as regional offices around the U.S., we deliver our members top-tier business intelligence and networking opportunities on a global scale. Learn more about TechAmerica at *www.techamerica.org* and CompTIA at *www.comptia.org*.

Follow us on:

GRANT THORNTON LLP

Grant Thornton's Global Public Sector, based in Alexandria, Va., is a global management consulting business with the mission of providing responsive and innovative financial, performance management and systems solutions to governments and international organizations. We provide comprehensive, cutting-edge solutions to the most challenging business issues facing government organizations. Our in-depth understanding of government operations and guiding legislation represents a distinct benefit to our clients. Many of our professionals have previous civilian and military public sector experience and understand the operating environment of government. Visit Grant Thornton's Global Public Sector at *www.grantthornton.com/publicsector*. In the U.S., visit Grant Thornton LLP at *www.GrantThornton.com*.

TechAmerica
Powered by CompTIA

Grant Thornton