

EXPANDING THE ROLE OF THE CIO:

Integrating Mission, Innovation, Technology, Services and People.



TABLE OF CONTENTS

Executive Summary	1
Federal IT Overview	2
Innovation	6
Cloud	7
Mobility	9
Program Delivery	11
Modular IT Development Strategies/Agile	12
Data Analytics	14
Cybersecurity	15
Continuous Monitoring	16
Privacy	18
Acquisition	18
IT Shared Services	20
Workforce	20
Conclusions	22
Appendix A - List of Interviewees	23
Appendix B - List of Interviewers	24
Acknowledgements	25
About the Sponsors	25

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 25 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, Grant Thornton has 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 http://www.pscouncil.org/c/p/CIO_Survey/CIO_Survey.aspx

Conducted interviews

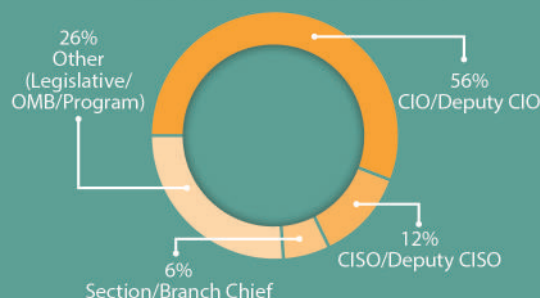
Dec. 2014–May 2015



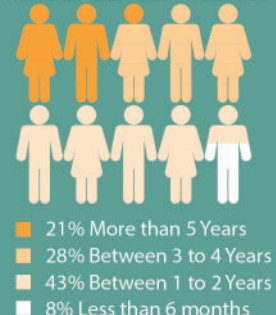
Interviewed

67 CIOs, CISOs, information technology management officials, and congressional oversight committee staff.

Interviewees by job function:



Time in Current Position:



EXECUTIVE SUMMARY

This is the 25th Anniversary of the federal government Chief Information Officer (CIO) community survey, sponsored and led by the Professional Services Council (PSC) and Grant Thornton LLP. In 2015, 67 information technology (IT) leaders participated, including **CIOs** of major federal departments and staff from OMB and Capitol Hill. Professionals from over 30 firms conducted the interviews.

The 25th survey of CIOs, CISOs, and key IT executives in the federal government saw the role of the CIO evolving into one that must not only support mission critical functions, but also expand to **address** innovation in providing services to meet that mission. Since our first survey, **IT** has progressed from mainframes, personal computers and floppy disks to a highly complex landscape of managed services, integrated mobile workforces, scalable technology and persistent cybersecurity threats.

Responding to the requirements of this new technology environment, in late December 2014, the Federal Information Technology Acquisition Reform Act (FITARA) was enacted. Aimed at making the CIO a more strategic player, these federal executives must now further evolve their tactics regarding how they integrate mission, innovation, technology, services and people. This year's survey reflects their ever **increasing role**. Our discussion is grouped around the top priorities and challenges faced by today's CIO: innovation, integration, protection and leadership.

In today's tight budgetary climate, CIOs are being called on to find innovative ways to use technology to perform operations faster and more effectively. Those we interviewed are looking to the cloud and modular development to help them achieve these results. All survey participants responded that their agency has adopted or is planning to adopt a **cloud-based solution**, but only 8% are where they want to be.

Modular development, especially based on the Agile methodology, continues to gain steam, with most CIOs reporting that Agile is being used somewhere in their organization. Some **Agile** projects are producing dramatic results in speed of delivery and customer satisfaction. In the area of mobility, more than half of those surveyed commented they were near or exactly where they want to be in regards to telework, but have a ways to go in being able to deliver digital services to their stakeholders.

As delivery of smaller, Agile applications are becoming more widespread, delivery of grand-scale programs are becoming the exception, not the rule, with good reason. CIOs explained that management of large IT programs "more often than not leads to cost overruns and schedule slippages."

When it comes to **data analytics**, government respondents expressed a higher level of confidence in the reliability and quality of their data than in the past, especially under the domain for which the data was created. However, they continue to report that their data is siloed and not easily accessible across the enterprise and across different domains.

It comes as no surprise that **cybersecurity** remains a top concern for those we interviewed. With the ever-increasing proliferation of networks, devices and applications, there has been a corresponding increase in both the number and sophistication of cyber threats. Twenty eight percent of respondents noted a 51-100% increase in cyber threats to their respective organization in the past year. Unfortunately, competing for the top cybersecurity talent to protect information systems continues to be difficult for federal agencies.

CIOs are also focused on the need to **streamline acquisitions**, adoption of shared services and workforce development. The adoption of category management is aimed at enabling the federal government to buy smarter and act more like a single enterprise by identifying core categories of spend, sharing best practices, and providing more streamlined solutions. To further stretch their resources, an overwhelming majority of CIOs we interviewed are currently using or plan to implement some form of shared services. CIOs are also taking the lead in building a future-ready workforce by adopting newer technologies aimed at attracting fresh, forward-thinking candidates.

It's clear from this year's 25th anniversary survey that CIOs and other federal IT executives are poised to become the innovative leaders of a future federal government that is more responsive, nimble and cost-effective than ever before in our nation's history.




FEDERAL IT OVERVIEW


TOP PRIORITIES


Each year, we begin the survey with an open-ended question to uncover the top priorities and challenges facing CIOs. Cybersecurity, revitalizing the workforce, modernizing the IT environments, acquisition, and mobility were cited as the top priorities.



 **CYBERSECURITY:** Cybersecurity remains the top priority for CIOs. The internal and external cybersecurity threat continues to evolve as the sophistication of “bad actors” increases. This requires continuous vigilance to protect multiple layers of technology across distributed endpoints and devices. CIOs agreed they have made great strides improving their detection of the threat, but caution agencies must continue to invest in recruiting and training a cybersecurity workforce to detect, understand and respond to the ever-changing threat. Better information sharing of the threat is also a priority.

CIOs should be asking the question, “How are we going to share threat and incident information to be able to anticipate, contain, and respond to attacks?”

 **REVITALIZING THE WORKFORCE:** CIOs remain focused on staffing the overall IT workforce with personnel who have the right skillsets. They acknowledge they must navigate through a number of challenges to do this, including: 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. One CIO noted the need to invest adequately in continuing to develop the top talent in the current workforce through effective training programs. CIOs also cited the need for continuous focus on attracting and retaining the technology workforce of the future as a crucial issue for the federal government. **For every federal IT worker under 30, there are 10 over 50**, and the average age of the technology workforce continues to increase. In addition, workers under 30 are significantly less likely to stay in the government for the long-term than their predecessors did.

 **IT MODERNIZATION:** Modernizing the IT environment remains another top priority among CIOs. CIOs are looking to better meet the needs of end users and change the structure around IT solutions. This includes increasing efficiencies by creating acquisition plans and business cases to drive new investments that reduce redundancies in the IT space. Yet, many agencies still suffer from an over reliance on legacy systems. As an example, the **Department of Defense spends approximately 80% on its legacy business systems and only 20% on developing the next generation of business solutions.**

 **ACQUISITION:** CIOs acknowledged the difficulty of keeping up with changing technology in a contracting environment that often limits flexibility and access to industry best practices and solutions. The federal contracting workforce has experienced tremendous turnover in recent years. **In fact, half of today’s federal contracting workforce has less than 10 years’ experience and half of this group, 25% of the workforce, has less than 5 years’ experience.** This, coupled with an incentive structure that is not always tied to mission results may in part explain why IT acquisition continues to be cited by CIOs as a top challenge. Many CIOs feel that restrictive contracting practices hamper the Government’s ability to take advantage of the innovative solutions that companies have to offer.

“Procurement contracts for services should be utilized in a manner that allows contractors the flexibility to provide the innovation and solutions that the Government needs to modernize their IT operations.”



MOBILITY: CIOs are committed to ensuring a seamless experience for employees who require “access anywhere, anytime.” One CIO noted that a “strong teleworking capacity is key to attracting and retaining talent, especially from industry and academia.” Most CIOs felt they had made significant improvements to enable their employees to work remotely. However, they qualified this by highlighting that employees typically conducted this work via government-issued laptops, not tablets or mobile devices. The next phase of activity is expanding the ability of employees to perform additional work functions on mobile devices. This will include making more legacy systems and applications mobile-enabled. CIOs also expressed that they had taken steps toward increasing how they interact with their customers through digital services and anticipated some breakthrough developments in this area in the next few years.

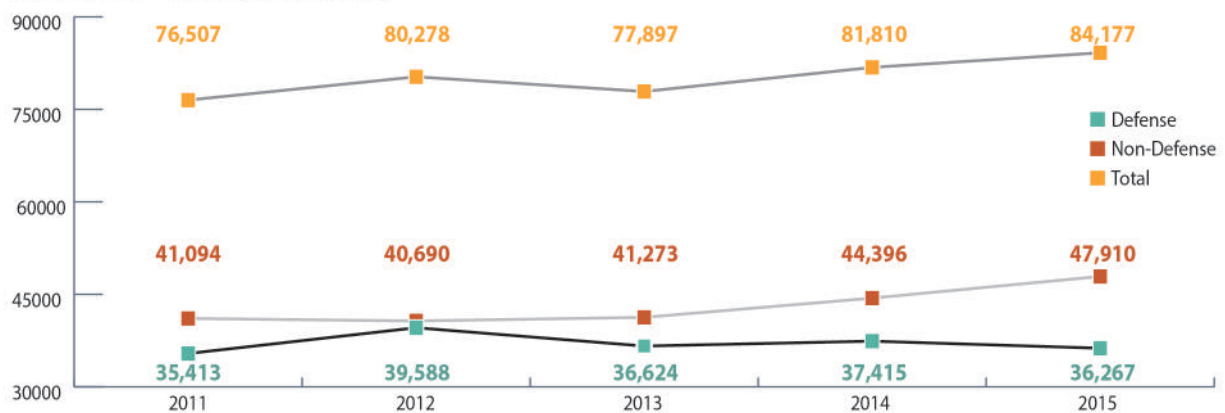
Respondents also identified other priorities, such as effectively spending Government money on IT contracts, increasing use of cloud services, implementing reliable, customer-focused technology, and executing a digital strategy. CIOs cited the flow of funding within the current budget environment, the culture and change management within each Federal agency, mobility, and governance as additional challenges.

HOW THE IT BUDGET IS BEING SPENT

The FY16 Analytical Perspectives volume of the President’s FY16 Budget Request, showed a \$2.4 billion, or 2.9%, increase in total Federal IT spending from FY14 to FY15. However, this growth was not evenly spread, with DoD IT spending dropping \$1.1 billion (-3.1%) but non-Defense IT spending growing \$3.5 billion (7.9%). Over the past 5 years, total federal IT spending has enjoyed steady, if modest, growth, with a 2.4% compound annual growth rate (CAGR) from FY11 to FY15 (which includes the substantial drop of \$2.4 billion (-3%) seen from FY12 to FY13.) But again, this growth differed greatly between DoD (.6% CAGR from FY11 to FY15) and non-Defense (3.9% CAGR).

The President’s FY16 Budget Request also included IT growth for FY16, with both DoD and non-Defense IT spending proposed to be increased by more than 2%. However, at the time of publication, disagreements between Congress and the President on spending levels prevent much clarity into where FY16 IT funding will ultimately land.

FEDERAL IT SPENDING (IN MILLIONS)¹



¹ In 2014 OMB’s Budget of the United States Government, Fiscal Year 2014, Analytical Perspectives, reported that the 2013CR defense spending was estimated at (in millions) \$38,810, non-defense was estimated at \$41,766, and the total funding amount was \$80,576. This was updated in the 2015 issuance to the figures above. Source: Budget of the United States Government, Analytical Perspectives, FY 2014, FY 2015 and FY 2016

NEW SPENDING VS SUSTAINMENT

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 operation and maintenance (O&M) on legacy applications and infrastructure. Like last year, several CIOs indicate they are spending more for DME than in previous years, but this estimate showed a modest decline over last year.

CIOs pointed out that it’s becoming increasingly difficult to segregate these items from one another. “Many of our smaller DME projects are being done in the cloud now, blurring the lines between DME and O&M.” When asked how they see the breakdown between O&M and DME in 3 years, all stated they expected to see increases in DME and declines in O&M. All CIOs agree that Portfoliostat has helped improve their understanding of IT spending within their organizations and felt this would continue to improve under FITARA. One CIO said he set a goal of reducing O&M and infrastructure spending to 40% in three years.

DME vs. O&M	2013	2014	FY2015	3 years from now
Development Modernization & Enhancement	15%	27%	25%	38%
Operations and Maintenance/Infrastructure	85%	73%	75%	62%

FITARA AND THE ROLE OF THE CIO

The Federal IT Acquisition Reform Act (FITARA) was enacted on December 19, 2014 and represents the most significant federal IT reform since the Clinger-Cohen Act of 1996. The proposed FITARA guidance aligns with the Office of Management and Budget’s (OMB) core objectives across the Federal IT portfolio to (1) drive value in Federal IT investments, (2) deliver world-class digital services, and (3) protect Federal IT assets and information. We asked CIOs to comment on how this new law would impact them and to also provide feedback on the OMB guidance released for comment in April 2015. CIOs across the board were supportive of the passage of the law and the guidance. Most felt that the law memorializes practices in governance and collaboration that are already occurring today. All CIOs also agreed that it will take time to fully understand the impacts of this law and felt that agencies will take different approaches to its implementation. As one might expect, the perspective on FITARA and how it should be implemented varied based on whether the CIO was at headquarters or within an operating component.



Federal IT Acquisition REFORM ACT (FITARA):
 Enacted December 19, 2014 and represents the most significant federal IT reform since the Clinger-Cohen Act of 1996 focused on:

- 1 Chief Information Officer (CIO) Authority Enhancements
- 2 Enhanced Transparency and Improved Risk Management in IT Investments
- 3 Portfolio Review
- 4 Expansion of Training and Use of IT Cadres
- 5 Continued Federal Data Center Consolidation
- 6 Maximizing the Benefit of the Federal Strategic Sourcing Initiative
- 7 Government-wide Software Purchasing Program

Federal agencies will need to thoughtfully consider what operations are best suited for consolidation at the enterprise level to ensure interoperability and operational efficiencies and what operations are best left at the local level to foster speed, manageable scope and customer engagement. Regardless of the exact distribution of enterprise vs. local work, FITARA will still help to provide CIO visibility and engagement on the pressing technology issues of the agency. The key to success will be to use FITARA to bring together all stakeholders in the C-suite to create an integrated IT budget approval process that all C-Suite stakeholders are part of, rather than the CIO creating a separate budget approval process.

Headquarter CIO

"We are hopeful FITARA will foster more collaborative discussion to improve communication and consensus on IT investments across the C suite."

"FITARA takes Clinger-Cohen to the next level."

"...started the right conversations. It will assist with providing more visibility into what is being bought. Policy changes have helped raise acquisition thresholds so more companies are able to be used in a more streamline[d] fashion."

"FITARA is the big change. We need the single point of authority."

Component CIO AND OTHER AGENCY EXECUTIVES

"While I get the intent, the intent and execution are two different things. Mission should drive decision-making on IT, not the CIO."

"It's good to have oversight but we don't want to lose agility."

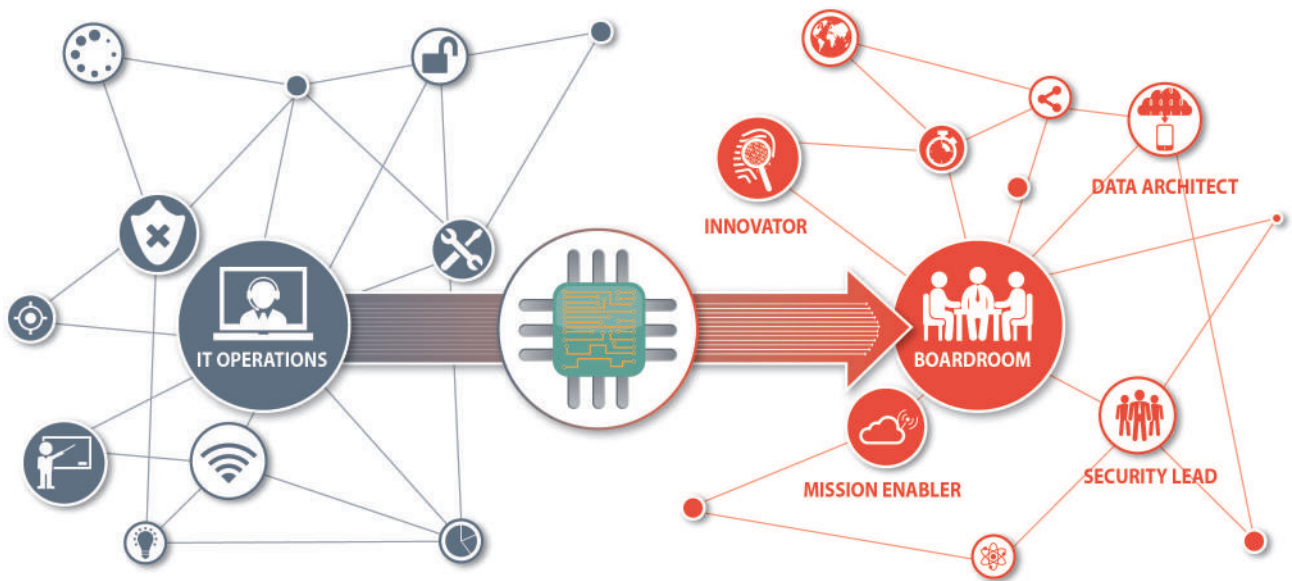
"Congress should be more aggressive with oversight of the laws that it passes. Only time will tell if this is successful."

"It's not clear what a good outcome will look like or how we will measure success."

"The guidance is less aggressive than initially enacted and this is good."

EVOLVING ROLE OF CIO

CIOs CONTINUE TO SEE THEIR ROLE CHANGING. CIO roles continue to vary across government, from an infrastructure/operations focus to driving strategic decision-making and using technology to help make innovation a reality across the enterprise. Many CIOs are focused on helping stakeholders access the information they need to accomplish the mission of the department. This in turn helps drive better decision-making. It was clear, though, that the only way a CIO can serve as a credible innovator and IT strategist is to ensure IT delivery is cost effective and operating as intended. One CIO commented, "Real authority comes from legitimacy, being able to deliver on what you say. This is the foundation for effective CIOs."



WHAT DOES THE CIO ROLE LOOK LIKE IN THE FUTURE? Most CIOs see a continued evolution. "The CIO role as it is defined today is not likely to exist [in the future]" one CIO remarked. "More investment is needed to incorporate IT into strategic business lines and management of the organization." Other roles such as Chief Risk Officer (CRO), Chief Data Officer (CDO), and Chief Technology Officer (CTO) can overlap with the CIO. Federal government agencies will need to consider how governance can better align IT services to business / mission objectives. The CIO must continue to play a role as an innovator who engages the business in how to use technology to improve service delivery and performance, an integrator who helps the enterprise blend technologies together across multiple platforms and contracts, and the leader who creates a team that helps the agency execute its mission.

INNOVATION

CIOs have a renewed focus on innovation to find new ways to use technology to perform operations faster and more cost effectively. CIOs cited innovation as a key tactic for successfully addressing tight budgets and resource constraints. So how are CIOs innovating? We heard a number of impressive success stories ranging from the development of new mobile apps using cloud-based platforms to finding better ways to analyze data to make decisions and protect the networks.

TOP AREAS OF IT INNOVATION



APPLICATION MODERNIZATION. One CIO said, “We’ve implemented new DevOps processes using Agile that have enabled us to get instant access to information it would have taken 6 months to see.” Another said, “We are moving legacy applications from the mainframe to the web. This will save us \$160M in people time by automating processes, enabling us to get supervisors from desks into the field.” This CIO acknowledged how hard it is to architect the web systems and relational databases to be as fast as the mainframe, but they’ve done this, and it’s paid big dividends.



DIGITAL SERVICES. Digital services is now becoming real. It’s been 2-3 years in the making. Now agencies are building their own digital services groups to identify other ways to serve their customers through the use of technology. The CIO Council is leading an IT solutions challenge which brings together a team of individuals who will work in small teams to solve IT challenges between now and September 2015. One such team is working to: “Create a cloud-shared services sandbox for all federal agencies to pilot technologies, develop applications, and model enterprise architecture.”² And we are just getting started.



IMPROVEMENTS IN DATA ANALYTICS THROUGH THE INTERNET OF THINGS. CIOs are also beginning to leverage the internet of things (IOT) to improve efficiency and save money. One CIO said, “We are leveraging IOT devices and better analytics to more effectively track and manage energy consumption. Using new devices enabled us to see situations where buildings had heaters and chillers on at the same time, and make adjustments to our systems to prevent this. This change has reduced energy consumption across the portfolio by 27%.” Many CIOs see IOT offering the potential for breakthrough performance in the coming years.



ADVANCES IN USE OF THE CLOUD. Leveraging the full capability of cloud-based development platforms was cited by some CIOs as an innovation that helps reduce costs. “We have used cloud to reduce our lifecycle development costs by 90% and bring applications to market in 70% less time.” Another CIO said, “Our move to cloud email has given our 17,000 staff back two hours per month where they don’t need to manage their email boxes and given them 400 times more storage than before.” Another said, “We have improved our DevOps efficiency through the use of a global cloud platform because our global organization can access hardware and software tools needed for development from a common application any place in the world.” Another said, “We can turn around an application in the cloud in a week, when it used to take months.” Cloud is here to stay.





INCREASED SOPHISTICATION IN CYBERSECURITY. A few CIOs cited cyber innovations. “We created a new Regional Security Stack system that reduced the overall number of security stacks from approximately 1,000 worldwide to just 50. This has enabled us to better defend ourselves while reducing costs.” Another innovation that will benefit government and the private sector involves advanced data standards for securely discovering and exchanging cyber threat information that will become available for improved network protection appliances and endpoint security tools. CIOs are eager for continued innovations in this area of growing concern.

“We have used cloud to reduce our lifecycle development costs by 90% and bring applications to market in 70% less time.”

² Alfred, Lori. “IT Solutions Challenge 2015 Problem Description: Lori Alfred – CIO Council.” May 15, 2015. Accessed May 16, 2015. <https://cio.gov/it-solutions-challenge-2015-problem-description-lori-alfred>

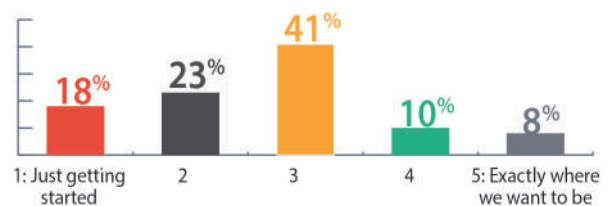
KEYS TO SUCCESSFUL INNOVATION include involving employees in identifying innovations, and putting in place policies that do not reprimand failure but rather encourage the pursuit of new ideas and methods. One CIO said, "It is my job to ... protect my team from anti-change criticism while they work to identify newer, smarter ways of doing things." One area where innovation is needed is acquisition, specifically Agile contracting. As the Professional Services Council's Acquisition Policy Survey reported in January 2015, while innovation was identified as a high priority for senior government acquisition leaders at OMB and the Department of Defense (DoD), the implementation of these objectives by the mid- and field-level acquisition workforce wasn't always occurring. CIOs agreed this was critical for continued innovation.

 <p>Barriers to Innovation</p> <p>CIOs acknowledged innovation isn't easy. "Individuals are afraid to try anything new due to oversight bodies (procurement, IG, Congress, GAO, etc.) due to the fear of failure." Even if fear wasn't a factor, it's simply challenging to get personnel to embrace a move away from the tried and true. Adding to these difficulties are the cuts departments have experienced to both budgets and personnel. One survey respondent said, "All the years of cutting have prevented the government from bringing in real expertise to drive the strategic vision for IT." It was suggested that CIOs have the ability to create "an innovation fund" which could be used to fund research and development into innovative ideas that can improve service delivery.</p>	 <p>Innovation Lessons Learned</p> <ul style="list-style-type: none"> • Move legacy applications to the web, enabling a mobile workforce • Leverage full capabilities of cloud-based platforms to reduce cost and increase efficiency • Create cloud-shared services for agencies to develop and use applications • Embrace innovation through modernized business processes and practices • Use contracting approaches that encourage industry to deliver new approaches and solutions
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


CLOUD

Four years after the push for rapid cloud adoption through the "Cloud First Strategy", agency cloud adoption is still slow, with only 8% of respondents indicating that they are where they want to be regarding their cloud adoption strategy. One CIO said, "We need a stronger strategy and vision that identifies how we can deploy more to the cloud securely and how it will benefit the organization and our stakeholders."

CLOUD ADOPTION PROGRESS

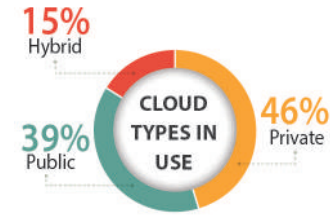


While many CIOs see cloud computing as a platform to accelerate the adoption of innovative development approaches and solutions, today most have only tackled the low-hanging fruit. "We've tackled the easy stuff, moving email and web sites to the cloud. Now, we are looking at how we can use a more Agile set of tools for application development in the cloud." Agencies are now looking for a common data platform that can provide them with infrastructure as a service, platform as a service, and software as a service. A number said they are beginning to pilot use of cloud-based development platforms to reduce costs while enabling collaboration by developers in multiple locations. CIOs believe that moving to cloud-based DevOps can improve speed of delivery and collaboration, and help automate processes like testing and verification, releases, and infrastructure updates.

 Benefits of cloud	CIOs who had moved to the cloud cited the following benefits			
	<ul style="list-style-type: none"> • Cost savings • Improved customer service • Faster access to data 	<ul style="list-style-type: none"> • Self-provisioning • Faster to stand up • Enhanced flexibility 	<ul style="list-style-type: none"> • Easier addition of services • Self-service • Enhanced collaboration 	<ul style="list-style-type: none"> • Faster application delivery • Improved testing, reliability and performance

CLOUD CONTINUED

IS PUBLIC, PRIVATE OR HYBRID THE BEST FIT? The types of cloud being used are mixed, and in part, reflect the nature of work being moved to the cloud. Forty-six percent of CIOs and CISOs surveyed use private cloud, 39% use public cloud and 15% use hybrid cloud technology in their organization.



DOES CLOUD SAVE MONEY? Interviewees had an appreciation of the potential cost reductions associated with moving to the cloud, but had mixed opinions about whether savings would be achieved by their agency. “Building out the use of commercial scale cloud capabilities will provide 70% cost reduction in hosting costs,” said one CIO. Another CIO said, “[There is] interest within the agency for moving to the cloud for budgetary reasons. However, the total cost of ownership remains unknown.” As we stated last year, rigorous cloud planning and an understanding of IT costing before migration are critical success factors in cloud migration.

SUCCESS FACTORS FOR CLOUD MIGRATION. “Cloud means something different to every person you ask. What are we actually trying to do by moving to the cloud? Are we getting better security with cloud? Are we saving enough money? Is this beneficial to resource management and utilization?” Survey respondents noted that you cannot underestimate the work needed to develop a strategy governing how to move applications to the cloud. Those who aren’t where they want to be are working diligently on developing a strategy that outlines what can be moved, the requirements and associated workload, supported by market surveys and detailed cost analyses to see how available solutions fit their needs. One CIO remarked, “We don’t know the opportunities of what we can do with the cloud. What does the interface look like? How do we manage the environment? How do we establish the security boundaries?”

It’s easy to lose sight of how cloud migration impacts users. “How will things be delivered to users? How much will it cost? These should be more important than where something will be hosted.” Another respondent pointed out migration is really a transformation effort and will require extensive change management.

“We have a challenge getting our Inspectors General (IG) to understand that in the event of an incident, they cannot knock down a door, shut down a server and take it. Email was tried in the cloud, but the IG stopped it.” The CIO Council can play a role in helping educate IGs and the Government Accountability Office (GAO) on how and why cloud makes sense to make it easier for CIOs to navigate through situations like that cited above. Another CIO cited the recent addition of the Cloud SIN on the GSA IT 70 schedule should simplify cloud acquisition.

“We are receiving good standard customer service at 1/6th cost of what we were paying before.”

Agencies across the federal sector agreed on the importance of establishing guidelines to procure cloud technologies (i.e., types of IT procurement contracts that are acceptable) and continue to utilize them in the future (i.e., guidelines around cybersecurity/data protection). One CIO advised, “They need to educate their procurement team on cloud and how to acquire it.” Another remarked, “Cost of licensing is going to proliferate out of control. We are creating a governance process to get this under control.”

“We need to become much more agile with respect to service delivery and continue to drive down costs by only paying for what we consume. Writing good contracts is the foundation for this.”

INTEGRATION CHALLENGES. Another CIO mentioned the integration challenges that can exist in certain cloud environments, such as the difficulty in integrating an asset management application with a different vendor’s financial system in their native cloud environment. The CIO is now contemplating bringing the asset management application back in house. Other CIOs commented on the integration challenges that can be experienced with cloud migration, such as single sign on, ensuring your software works on provider’s platform, application rationalization – what can and can’t go – and capability to manage millions of transactions per day without performance degradation. Another said, “Harder than we thought. We may see savings down the line but it’s too early to know.”



ALL CLOUD PROVIDERS AREN'T CREATED EQUAL. "The incident response for the Cloud through our vendor (one of [the] top providers) has not been as responsive as expected for certain problems including Personally Identifiable Information (PII) and malware. We need real-time support. If an incident occurs, we submit requests in the form of tickets to our vendor who in turn identifies someone to help provide a solution. In several instances, we know more information than they do as they are more accustomed to selling and not incident response." "There isn't an advantage of going to the cloud since the support is now outsourced which can cause slow response times and inadequate support." "We haven't seen any benefits yet. We are leasing services through the department and finding it a challenge to manage services and costs." "No federal cloud will be capable of doing what commercial cloud providers will do in five years. Established providers offer the latest technology and security at competitive prices."

"We need to become much more agile with respect to service delivery and continue to drive down costs by only paying for what we consume. Writing good contracts is the foundation for this."

APPROACHES TO CLOUD SECURITY. Cloud security is a top concern. Oftentimes organizations are hesitant to adopt certain cloud technologies due to perceived data security concerns. A means to overcome federal agencies' data security concerns could be to examine organizations' internal private cloud security regulations. One respondent stated that to overcome data security concerns related to the cloud "[we] need to be aware of cybersecurity; [and that] different data requires different security." One CIO said, "100% of our cloud is currently private. From a policy perspective, this translates into everything being treated as "High," or to the level of top secret material. No one else does this and [this] needs to be reexamined." It is encouraging to note that commercial cloud implementations like the ones at CIA and other intelligence activities are dispelling myths around security and helping to focus the debate on ensuring the right level of security for each situation. Data needing extra attention and planning includes PII and classified information. How do we manage PII in the cloud?

"It's easy to say 'cloud first' but there are many steps that need to happen before the initial barriers can be breached."



- Establish a risk-based security model based on the data that is stored
- Do a total cost of ownership assessment on potential cost savings
- Be a diplomat. Moving is 80% about people involved, and 20% about technology
- TIC, FISMA, FedRAMP, NIST, CDM* and other compliance activities need to be integrated in cloud offerings
- Build in transition paths from cloud service providers (public and private) to ensure the ability to simply transition from one provider to another without significant transition costs
- Don't short-change planning and ensure you develop very clear SOWs with models to pay based on consumption, clear accountability and recourse if things don't end up as planned
- Establish a very clear roadmap and governance
- Don't assume the integration will be easy; assess application compatibility

* Trusted Internet Connections (TIC), Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), National Institute of Standards and Technology (NIST), Continuous Diagnostics and Mitigation (CDM)

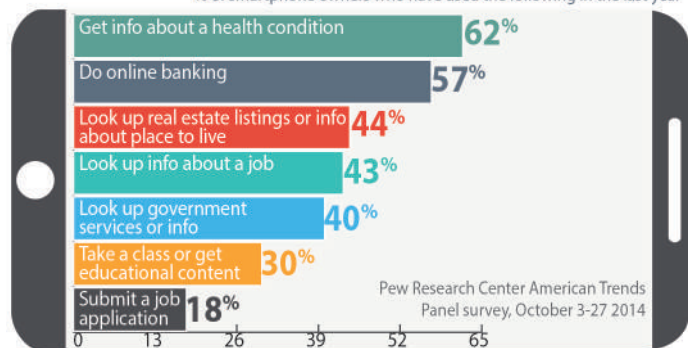
MOBILITY

The proliferation of mobile devices and demand of citizens for access to services online anytime continues to grow. A recent Pew study cited that **40% of smartphone users had looked up government services or information online**, and 43% looked up information about a job. Forbes reported there was a 26% increase in telework between 2013 and 2014. One CIO commented, "work is what we do, not where we are." So how do CIOs gauge their ability to enable employees and citizens to work in this mobile world? It depends.

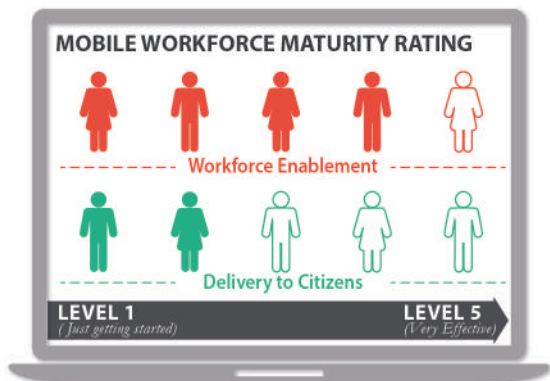
Agencies have made advances in telework, with more than half commenting that they were near or exactly where they want to be in mobile enablement of their workforce.

MORE THAN HALF OF SMARTPHONE OWNERS HAVE USED THEIR PHONE TO GET HEALTH INFORMATION, DO ONLINE BANKING

% of smartphone owners who have used the following in the last year



MOBILITY CONTINUED



“Mobile maturity level is trending positive,” one CIO noted.

Another commented, “[Our] entire organization is remote, all telework – [we] have people in all 50 states.” Others responded that they are making progress with mobility efforts, but “cannot fully adopt a mobile workforce until changes are made to increase hotel options.” Culturally, they notice that the younger generation requires mobility, while older generations are having a hard time adjusting. CIOs also expressed concerns around management, stating that teleconferencing is not yet seamless and productivity and performance are still hard to judge.

Resolving issues around teleworking is important for the future.

One CIO noted, “Strong teleworking capacity is key to attracting

and retaining talent, especially from industry and academia.” But it’s not just staff who expect work-from-anywhere flexibility, customers do as well. “... [the] industry and customer is driving us that way. Can’t be tethered to the desk... need the ability to always work... and buy it as a service.” Another CIO said, “Mobility has saved [our] organization \$30M per year. We don’t have to wait on people to come back from sick leave or wait on alternate work schedules. We keep things going – snow days don’t matter and we can be closer to customer, and hire talent wherever they reside.” CIOs want and are helping to achieve a mobile, resilient workforce that is self-provisioning and can access critical systems securely.

LAPTOPS VERSUS MOBILITY. As we analyzed the discussions, it was clear that remote enablement is accomplished primarily through secure laptops, and most agency employees can’t yet do the majority of their work securely from tablets or phones. “Mobility is different than desktop,” said one respondent. Another said, “We are really good at it conceptually, but our systems haven’t caught up. For example, the quality of our VoIP is not good; therefore, it’s not used. We still have some ways to go to get the tools we need.”

Video conferencing is sometimes used, but not used across all agencies. Many agencies are comfortable with collaborative meeting spaces but don’t have an enterprise approach. CIOs envision continued improvements in mobile enablement of legacy applications for employees using tablets and mobile devices, but they aren’t there yet. We will continue to see a push for mobility maturity, along with of the government’s enterprise systems, and app development capabilities. Agencies want a mobile, resilient workforce in the future to access business-critical systems from anywhere with key pieces of equipment. “We need access to data from any place and any time securely. Legacy apps don’t behave well when you are mobile, and it shouldn’t matter.”

DIGITAL SERVICES COMPETENCE is in its nascent stage. Externally, CIOs agree they can’t do business with customers and citizens electronically today at the level of maturity they desire. “Allowing our customers to get business done with us in a mobile-friendly fashion? We’re not there yet,” said one CIO. “Customer lifecycle journey is in process. Systems are still browser-based ... [we’re] still [in] the 90s world.” Customers want to see more apps for phones and tablets and view government websites on-the-go. Even search engines are creating algorithms to return results on a mobile device based on how mobile-friendly the website ranks. Agencies are experimenting with creation of mobile apps and app stores. It seems there could be a greater opportunity for sharing what’s being done across the government. Another respondent said, “we should stay out of [the] application-writing business but [we] need mobile tools.” Agencies overall responded that they need better mobile platforms and more effective strategies and tools and data control but that it can be hard to break out of legacy systems.

“Our agency has developed many apps. The issue is not app development, but app utilization,” one CIO commented. “How is the mobile platform being used effectively and does it change the customer outcome? We’ll see more mobile demand for increasing how we interact with our customers but [we] need to do a better job of understanding customer/user needs and experience before we develop apps that we assume they want.” Recent OMB policy requiring CIOs to create digital services groups has created significant buzz and focus on this area, and CIOs are confident they will make strides here in the coming year.

Challenges are present in the drive for mobility as well. CIOs reported on mobility roadblocks such as data security, vulnerabilities in personal devices, cultural shifts, and realizing the payoffs. Today, employees are demanding access to

information and people from anywhere at any time. Successfully addressing the need to do trusted computing from untrusted devices will be a crucial next step in raising the bar on cybersecurity while ensuring the flow of information required for mission results.

Where do they expect to be in 3 Years?

- Anywhere anytime having access to the data and tools you need
- Whatever is shared is done appropriately
- Convergence of mobile experience with desktop/laptop
- Improving security management of mobile devices, creating more structured support
- Better mobile enablement of legacy systems
- Increases in ability to serve citizens and customers through digital services

Biggest barriers to REACHING Mobile Excellence

SECURITY

- More effective authentication and trust relationships
- Better protection of data in transmission and at rest

TRAINING

- Education of users on effective use of mobile devices
- Broadband limitations in areas where certain offices and customers exist
- Financial resource limitations
- Acceptance from older workforce

DATA MANAGEMENT

- Data access and retention issues need to be resolved to better enable telework
- Data not on the network being stored on hard drives needs to be captured and stored better in order to become more mobile in the coming years
- Proper wireless capacity sizing

SKILL LIMITATIONS

- Mobile application development competencies
- Mobile Security
- Mobile architecture

HOW ARE YOU ADDRESSING PERCEIVED SECURITY Challenges of Mobile?

<ul style="list-style-type: none"> • Containerization of data based on risk level with associated policy and rules of behavior. • Better recognition of nature of information on mobile devices, and not overdoing protection based on low risk 	<ul style="list-style-type: none"> • New platforms for software tokens for certification and accreditation • Encryption, not commingling personal and business email/data 	<ul style="list-style-type: none"> • Better development and adoption of policies and governance • Mobile Device Management (MDM) to enable enforcement of security standards and 	<ul style="list-style-type: none"> • configurations, protect data on lost devices by being able to remotely wipe the device and provide reporting capabilities for what is on the devices
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

PROGRAM DELIVERY

“Ninety-four percent of large federal information technology projects over the past 10 years were unsuccessful — more than half were delayed, over budget, or didn’t meet user expectations, and 41.4 percent failed completely.”³ With that sort of track record, it is no wonder CIOs agree that grand-scale federal IT programs are often fraught with risks and nearly impossible to implement without failing. CIOs stated that large programs like healthcare.gov are working on trying to achieve an almost impossible task: “elicit coordinated, purposeful action from a collection of entities that don’t know each other, don’t trust each other, have conflicting objectives, and face diverging incentives.”⁴

Another CIO said, “we focus on [the] latest and greatest technology – without thinking about the change management... if users don’t like it, they won’t use it, and then you have failed. We fixate on the flash and glamour... IV&V change management and governance are just as important.” CIOs identified the following top reasons why large federal IT programs fail:

Biggest Challenges to delivering large IT programs

<ul style="list-style-type: none"> • Unclear, unachievable business requirements • Poor user engagement and buy in • Underestimating business process change • Inadequate planning 	<ul style="list-style-type: none"> • Ineffective governance • Lack of skills/inconsistent level of experienced program managers • Poorly constructed teams • Ineffective communication 	<ul style="list-style-type: none"> • Miscalculating integration challenges • Inadequate scope management • No clear definition of success or success measures 	<ul style="list-style-type: none"> • Misjudging change management • Acquisition changes/contract limits • Poor business/mission leader and technology leader alignment
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3 New York Times. Johnson, Clay, and Harper Reed. "Why the Government Never Gets Tech Right." 24 Oct. 2013. Accessed 5/31/15. http://www.nytimes.com/2013/10/25/opinion/getting-to-the-bottom-of-healthcaregovs-flop.html?_r=1
4 Forbes Magazine. Woodhill, Louis. The Obamacare Website Failed For The Same Reason The Soviet Union Did. 13 Nov. 2013 Accessed 5/31/15 <http://www.forbes.com/sites/louiswoodhill/2013/11/13/the-obamacare-website-failed-for-the-same-reason-the-soviet-union-did/>

PROGRAM DELIVERY CONTINUED

Most CIOs acknowledged the scope of large IT projects and the ability to manage them was the biggest challenge. The requirements and needs of customers

“Watermelon projects. They look green on the outside but they’re red inside. Everything looks great until you deliver and then it blows up.”

of large IT solutions inevitably change over time and the larger an implementation effort is, the more this introduces vulnerabilities, which can result in mismanagement of risks, costs and schedules. CIOs believe that clear contract requirements in combination with proper management of performance-based contracts could set clear paths for success in incremental deliveries. Ensuring you have an adequate, honest approach for evaluating the health of large programs is also critical to know if you have what one CIO called, “Watermelon projects. They look green on the outside but they’re red inside. Everything looks great until you deliver and then it blows up.”

CIOs also identified that large IT projects and weak contract / project management are closely related to finding enough experienced program managers. The Project Management Institute’s (PMI) Certified Project Management Professionals (PMP) are sought after as noted by a respondent who expressed interest in adding PMP-credentialed resources to their agency’s talent pool. These certifications and programs are very valuable, but the challenge with all such programs and certifications is to ensure those certifications can be supported by experience, commensurate with the needs of the program. “We have major and minor investments. Major are supposed to be level 3 certified, but we do not have 24 PMs to manage those.” As described by one respondent, “We didn’t start with the strongest base of project management skills and we’re continuing to evolve from that foundation, including agile project management.”

So how are programs being developed? Most CIOs are working to make large programs a thing of the past. According to one CIO, “large federal IT contracts are becoming the exception, not the rule.” In 2012, OMB identified shortcomings associated with the “grand-design” IT development approach and recommended an alternative solution, aimed at reducing government investment risk and financial exposure. In its “Contracting Guidance to Support Modular IT Development,” OMB presents the modular approach to the development lifecycle and the anticipated results. Most CIOs are working diligently to move to an agile approach. One CIO said, “We break large programs into smaller projects [under] \$1M [and in] 5 to 6 month [increments].” They also cited a number of other best practices. One CIO said, “Focusing on soft risks, like stakeholder adoption and ownership is critical and doesn’t always get the emphasis it needs.” CIOs also said they can’t be afraid to cancel projects when things aren’t going well.

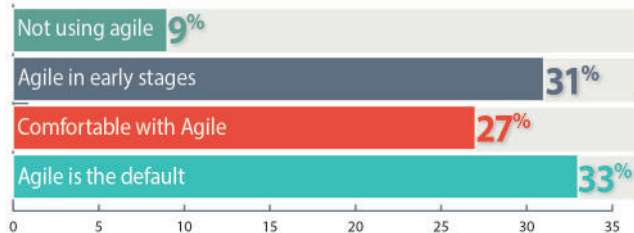


- Using modular/agile development
- Building risk incentives into vendor contracts
- Continuous incremental testing
- Increasing management attention on project and program health at regular intervals
- Integrated investment review boards that align business and C suite
- Structured program and change management tools and processes
- Cancelling projects that are in danger of failing
- Hiring experienced, well trained, certified PMs
- Project health dashboards/ Clear metrics (adoption, value, impact, utilization)
- Service level agreements
- Customer engagement throughout development/testing

MODULAR IT DEVELOPMENT STRATEGIES/AGILE

Increasingly, Agile delivery techniques are being used to address large IT project challenges and to deliver usable functionality and value in a modular, adaptive fashion. Valuing the method’s emphasis on communication, demonstration, feedback, iteration, and working software, CIOs are steadily moving towards Agile. 91% of CIO respondents report some form of Agile adoption.

PROGRESS IMPLEMENTING AGILE



In many cases Agile adoption is emergent; only one-third of surveyed CIOs report that Agile is their default methodology. Agile usage varies from agency to agency. Some agencies are working to pilot the method; others have established

proven team-level agile practices and are now working to use Agile at scale. One respondent noted the benefits of Agile stating, **“47% of the projects on the OMB dashboard are using Agile, and have seen an average decrease in delivery time of 21 days.”**

“Now we are running the projects in a very different way and seeing dramatic results in the speed of delivery and customer satisfaction.”

Citing uncertainty and innovation conservatism, respondents report a reluctance to fully adopt Agile. One CIO said, “We are concerned about innovation and moving into anything other than established business processes. Individuals fear failure and oversight organization (IG, Congress, GAO, etc.) repercussions.”

When asked about Agile lessons learned, CIOs site the importance of Agile training and skillset development, industry expertise, coaching, metrics, management reporting, Product Owner involvement, and OCIO and business unit collaboration.

“Agile development in a traditional procurement world is challenging”

Use of iteration – to balance feature, resource, and schedule decisions – was also reported as an important lesson. On this topic, one CIO stated: “I would say our failure of acting as our own system integrator, is our biggest challenge. By breaking up the work, we are able to see smaller failures, which are far easier to manage.”

Some agencies are expanding the use of Agile, beyond IT, into other management domains, such as operations and acquisition. For example, one CIO stated: “Rather than sending out a Request for Proposal (RFP) with a list of [system] requirements and getting responses back that don’t really work for us, we are aiming to have a more agile approach.”

Increasingly, CIOs acknowledge that solutions cannot be totally defined up front. CIOs are using Agile to shift focus from adherence to predictive plans to delivery of value. Many respondents report that they are forgoing up-front development of comprehensive requirements specifications. Instead, Statements of Objectives (SOO) and similar acquisition techniques are being used to encourage agility and innovation, to improve IT investment value, and to increase IT return on investment (ROI).

Agencies at the vanguard of Agile adoption have set their sights on improving acquisition agility. This thinking is consistent with oversight organization guidance, such as the Capital Programming Guide, which states: “Agencies should, to the maximum extent possible, consider breaking large acquisitions into smaller, more manageable segments or modules. Each module should be economically and programmatically viable (i.e., useful).”

Despite guidance aimed at improving agility and progress on this front, CIOs report that acquisition challenges remain.

“By breaking up the work, we are able to see smaller failures which are far easier to manage.”

Respondents advise that traditional procurement and contract management practices do not fully support Agile IT delivery methods. Moreover, survey responses indicate that adoption of Agile acquisition practices has proven difficult, especially where acquisition professionals are tenured and there is a reluctance to change entrenched business processes.

Top Challenges Implementing Agile

- Inadequate Agile training; nascent understanding of Agile critical success factors

- Role and responsibility confusion; organizing OCIO, business unit, and vendor team members
- Inadequate management rigor; ineffective use of metrics and performance analytics

- Lack of DevOps; poor communication, collaboration, and automation of IT functions
- Entrenched acquisition practices that do not fully support adaptive IT delivery

- Establish disciplined, smart, simple, standard agile practices and train teams
- Collaborate and communicate; increase interaction between developers and Product Owners

- Define ‘Ready’ and ‘Done’ to ensure that stories are complete, understood and implemented correctly
- Steer development toward demonstrable value, not adherence to predictive plans

Agile Best Practices

- Measurement drives action and focus; use inspect and adapt metrics to drive improvements

To overcome this reluctance, respondents report that agencies are experimenting with contracts that organize Agile work within contract line item numbers (CLINs) that allow for iterative delivery and inspection and provide the flexibility to limit long-term commitment to [potentially underperforming] contractors.

With regularity, oversight organizations, like GAO and the OMB, express concern about expansive federal IT programs that have taken years and failed at alarming rates. Importantly, CIOs understand that Agile is no 'silver bullet.' Agile is a useful technique – one that complements management competence.

“There is a great fear of failure and we are trying to determine what can be done to change the mindset of individuals to become more open to change.”

DATA ANALYTICS

Data analytics continued to be an area of focus for federal CIOs. While respondents discussed the progress they have been able to make over the past year, they continued to encounter challenges to fully realizing the benefits of mature data-driven capabilities.

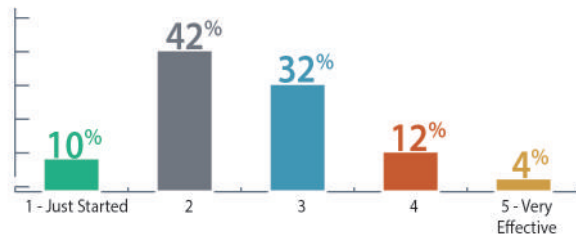
The level of data management maturity varies across federal agencies. Those that employed more mature processes indicated that they were able to use data to drive business decisions. With over 80% of respondents noting that their data-driven capabilities were in the early stages of maturity, these agencies identified the need for help in managing their data and developing a data strategy. Successful data management programs usually include strategic plans that align with the agency's mission and business strategies. Executive leadership involvement and support are also key, along with having an established governance structure to guide and prioritize data activities and establish policies and regulations for managing the data.

Our respondents expressed that in recent years, efforts have led to improved data quality; however, they indicated they had a long way to go. Challenges expressed included siloed data not easily accessible across the enterprise and across domains. According to a recent **Federal Times** report, by 2024, agencies will spend \$16.5B storing redundant data that they won't use.⁵

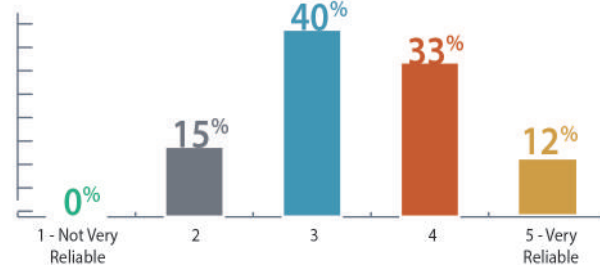
“The common misconception is that through the purchase of a data warehouse agencies will automatically be able to gain meaningful insight into the data. It needs to be recognized that in order to leverage this tool properly, knowledgeable people are essential to maximizing its benefits.”

This can lead to the inability of agencies to easily merge various data sets to assess new scenarios, address broader questions, and report at the department level. So even if data creation and processing at the transaction level was under control, improvements are still needed. CIO participants indicated that they would like to serve their user communities better. In order to achieve this goal, they want to improve their data offerings so that users are spending less time cleaning and organizing their data and more time analyzing and garnering intelligence from their data. Agencies are leveraging Master Data Management (MDM) to help achieve this goal. MDM is the implementation of policies, procedures, and technology to define, conform, and distribute a uniform and consistent representation of the key data concepts throughout the enterprise. Data concepts that are commonly mastered include chart of accounts,

MATURITY IN ABILITY TO LEVERAGE ORGANIZATIONAL DATA TO DRIVE KEY BUSINESS DECISIONS



RELIABILITY OF ORGANIZATION'S DATA



they won't use.⁵ This can lead to the inability of agencies to easily merge various data sets to assess new scenarios, address broader questions, and report at the department level. So even if data creation and processing at the transaction level was under control, improvements are still needed.

CIO participants indicated that they would like to serve their user communities better. In order to achieve this goal, they want to improve their data offerings so that users are

5 Stone, Adam. "The Path to Smarter Data Center Consolidation," *Federal Times*. Editorial white paper. Accessed: 2/25/15. <http://hub.federaltimes.com/whitepapers/11202014-smarter-data-center-consolidation-3215PS-5843CL.html>

products, vendors, customers, etc. Most respondents are looking to the Department level for guidance around MDM, and some are waiting for MDM implementations at the agency level. MDM is mentioned as being critical to Open Data initiatives, data accuracy programs, and improving effectiveness of analytics solutions.

Open data and data transparency are another common topic mentioned by agencies as demands for data access increases and legislation such as the DATA Act are enacted. One CIO suggested, “[We] need to make data accessible; make it uniform to look at collectively integrating/consolidating data warehouses; consolidating and collapsing, data mashing from multiple related data sets.” CDOs are gaining presence in government agencies and are expected to drive this along with other data management objectives. Even so, 67% of respondents indicated that the CIO is involved in preparing for the DATA Act and providing OMB and Treasury with feedback on the initiative. Respondents noted that increased transparency and easy access to data provides for increased insights, but also raises privacy concerns.

AGENCIES WITH MDM IMPLEMENTATION PLANS



What Agencies Are Doing To Improve Data Analytics:

- Visualization
- Meta data model development
- Enterprise data management strategy
- Digitization with hyperlinks
- Converting PDF docs into searchable html
- Open data – mashing data
- Data governance improvement
- Improved archiving and retention processes

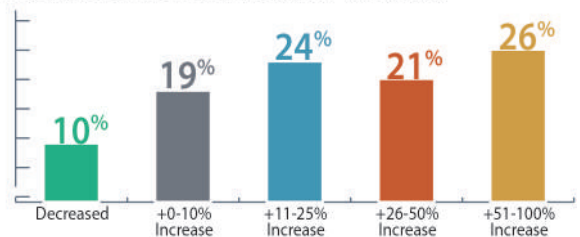
CYBERSECURITY

The public sector experienced nearly 50 times more cyber incidents than any other industry in 2014.⁶ It is no surprise, therefore, that cybersecurity remains the top priority and challenge for CIOs and CISOs. Socially engineered spam, phishing, spyware and other external threats from cyber criminals, nation states, and rogue actors are more sophisticated and persistent than ever before. 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.

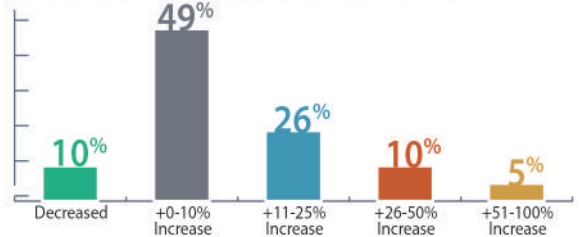
The traditional methods of boundary protection are no longer sufficient. Cybersecurity must address verifying risks from multiple threat vectors across a multitude of networks and devices inside and outside an agency. Ninety percent of CIOs surveyed experienced an increase in cyber incidents in 2014. Twenty-eight percent reported a 51-100% increase in cyber threats. A number of CIOs pointed out that the increase in threats could be due to having more effective approaches and tools to monitor and track such threats.

Cybersecurity spending is increasing too, but not proportionally to the increase in threats. From our results, 10% reported a decrease in cybersecurity spending, and 44% of CIOs cited a moderate increase of 0-10% in cybersecurity spending. As a result of this trend, CIOs are prioritizing buying innovative security tools, recruiting top talent and increasing agency-wide security awareness.

INCREASES IN CYBERSECURITY THREATS



INCREASES IN CYBERSECURITY SPENDING



6 Verizon 2015 Data Breach Incident Report

CYBERSECURITY CONTINUED

One of the main challenges echoed by CIOs in this year's survey was attracting top-tier security and privacy talent to the federal government. One of our interviewees attributed this dilemma to the "Talent War." There is a difficulty across agencies in the federal sector to attract top talent because of limits on compensation and time to hire. Respondents pointed out that it is almost impossible to compete with the commercial sector which can offer much more lucrative salaries with bonuses. There is an on-going war for talent, and these impediments for the government are a significant hindrance. Issues about compensation caps similarly hinder government contractors' ability to compete with the commercial cybersecurity market. There was also a level of concern with the current interview and hiring process and its ability to distinguish talent.

Due to spending restrictions, interviewees suggested shifting agency focus to metrics and tool innovation. Integrated security metrics shared across agencies will help identify trends and mitigate risks using shared services and resources. Interviewees suggested dashboards so senior executives have a better understanding of risks and can escalate issues to the appropriate stakeholders. The increase in collaboration with the CIO and the utilization of new tools will help agencies address their cyber threats in a tight budget environment.

While it is encouraging to see best practices like common security architectures, continuous monitoring, etc., being implemented, the need still remains to allow the rapid adoption of new approaches and ideas that will raise the bar on security while still allowing information sharing with unanticipated users and the ability to use untrusted devices for trusted computing.

The public sector experienced nearly 50 times more security incidents than any other industry.

Cyber criminals and bad actors possess the resources to create a more sophisticated and persistent threat than ever before.

(Source: 2015 Verizon Data Breach Incident Report)

Most Common Cybersecurity Threats



- Phishing/Social Engineering
- Spyware/Malware
- RAM scraping
- Credential Issues

Detecting, responding to and recovering from these threats is better but requires continuous improvement in a number of areas:

- Trust/Credential technology and management
- Common cyber data model
- Interoperability among cyber tools

- More integrated toolsets
- Reduction of technology insertion issues with integrated tool sets
- Better cyber metric dashboards



Cybersecurity Best Practices

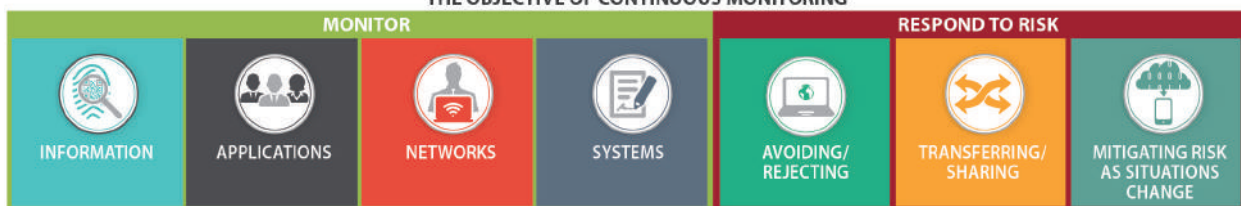
- Sharing of real-time threat information
- Increased automation of defense systems that can respond in real time
- Interoperability of tools
- Improved trust – both authentication and organizational trust

- Layered, adaptable defense systems that communicate, interoperate, and automate defenses
- Cloud-based threat analytic and reporting solutions
- Role-based behavior analysis to track and identify potential insider threat behaviors

CONTINUOUS MONITORING

The National Institute of Standards and Technology (NIST) defines continuous monitoring as maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions. The objective of continuous monitoring is to monitor an organization's information, applications, networks, and systems and respond to risk accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change. From our interviews, we noticed a common trend of responses stating that continuous monitoring / continuous diagnostics and mitigation (CDM) has gotten off to a fast start but has not yet realized its full potential. CIOs have utilized a number of commercial and agency-specific tools to automate their monitoring, management, and remediation control of information and data flow and storage.

THE OBJECTIVE OF CONTINUOUS MONITORING



Continuous monitoring provides a broad range of benefits to federal agencies. First, it creates better awareness of cyber-security and privacy in terms of knowing risks/vulnerabilities at early stages to minimize damage and remediate security risks. Continuous monitoring provides visibility into assets and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls and implement prioritized remedies. Respondents stressed the importance of replacing the every three-year assessment process of information systems under FISMA. This old process resulted in out-of-date security information and increased risk in vulnerabilities. Over the next year, CIOs expect continuous monitoring to have a greater impact through automated assessments, up-to-date information/data and immediate vulnerability detection and remediation.

“There is no one-stop shop, but a large, diverse set of tools is needed to identify risks.”

It is evident that continuous monitoring is vital for the mitigation of security risk, but there are still some issues and challenges. First, in order for continuous monitoring to flourish, this must be a priority for the agency from a budget and resource

perspective. Another challenge is the integration of CDM with other agency initiatives and operations as most current federal tools are DHS-specific and oftentimes tailored to DHS’ mission. As new tools are developed and agencies continue to collaborate, CDM and continuous monitoring should only expand in terms of agency use and government impact.




- DHS Scanning/vulnerability analysis & behavior-based tools (CDM platform)
- Sim Tools (Nessus)
- Tenable CDM tool
- McAfee suite
- Cyber Security Monitoring and Operations (ECMO)

- RSA Archer Governance Risk and Compliance (GRC)
- Q1 Radar
- HP OpenView
- GroundWork
- NetIQ
- HP WebInspect

- HP SiteScope (end-to-end monitoring)
- FireEye
- Blue Coat
- BigFix
- Tivoli (IBM) tool
- ForeFront

- Improves agency awareness of current / upcoming security vulnerabilities and threats
- Visible real-time data of their agency's network, end points, cloud capabilities, security, privacy and other information
- Improves compliance with NIST & FISMA requirements/controls
- Provides high level dashboards outlining security safeguards and current status

- Alleviates extensive assessments conducted every few years, which lead to outdated security/privacy information
- Higher need for trained resources to implement, control and oversee the CM process
- Use of automated process/control, highlighting critical information for the agency
- Helps top-level management make cost-effective and risk-based decisions supporting their agency-specific missions



--- IMPACTS OF ---
Continuous Monitoring

CONTINUOUS MONITORING *Lessons Learned*

- Share issues / successes within continuous monitoring/CDM across all government agencies
- Agencies need to prioritize training and awareness so employees can understand the CDM process

- Taking into consideration budgetary constraints, there is a challenge to determine appropriate levels of risk to accept while still protecting data
- Increased need to pick the right tool / vendor for CDM, ensuring the tool is in

- compliance / sync with agency missions / goals
- Prioritize proper / clear reporting of CDM data within management and across agencies going forward

PRIVACY

As agencies expand and become more mature from an IT perspective, the necessity for proper security safeguards of personal identifiable information and data is increasing. Many of the respondents stated their main privacy priority is to accurately reconcile OMB guidance with NIST processes to delineate responsibilities with the Chief Privacy Officer. Agencies have adopted “privacy core groups” to understand general counsel and OMB requirements as well as implementation methods. These core groups also are in charge of leading privacy training to spread awareness in their agencies.

Agencies are facing challenges when it comes to the issue of privacy. First, many respondents said there are current issues with the infrastructure and organization structure. For example, some agencies have separate privacy offices, which brings up an issue of integration. Next, some agencies have not appointed a Chief Privacy Officer. Without proper delegation, the importance of privacy is diminished at the agency. In addition, CIOs are having issues deciding how, when and what data to share. It is important for the privacy offices to explain the need to share certain data and the acceptance of the risk that comes with data sharing. Finally, a key theme from our responses was the need for a general and automated system for privacy safeguards. From a reporting and risk-mitigation perspective, an automated tool or system is a priority for many agencies.

ACQUISITION

CIOs and CISOs identified multiple changes that need to be made to the acquisition process, to include a more streamlined acquisition approach, increased flexibility and accessibility of contract vehicles, and faster ways to adopt new technology. Acquisition is one of the largest problems, as it delays access to technology.

A key challenge identified in the survey is that contracting officers often work independently from program management teams. With a lack of aligned incentives and competing priorities, this fragmentation of the “acquisition team” results in the misuse of LPTA, reliance on rigid statements of work and limited adoption of alternative approaches and best practices – all to the detriment of getting the best results for the government.

Agencies continue to face budget uncertainty and limited acquisition resources. While much still remains to be done to bring speed, agility, and innovation into government IT contracting, this year’s survey did identify some improvements being made. Organizations are looking to make systematic changes that provide new operating models to meet agency needs, managing suppliers while still giving them the flexibility to innovate, and ensuring acquisition professionals use data analytics, market demand, user requirements, and acquisition strategies that help deliver better results and ensure customer engagement.

“Something that benefits one agency should benefit all government agencies.”

To help improve the acquisition process, OMB is exploring practices to address different aspects of the procurement lifecycle, including the Acquisition 360 program. This transaction-based feedback tool allows agencies to identify strengths and weaknesses in their acquisition processes with the focus on pre- and

post-award activities and contract execution. Some agencies have taken a different approach by investing in vendor management offices to help identify, implement, and sustain specific strategies to reduce cost and create value by working collaboratively with IT vendors. Additionally, OMB is offering low-cost training opportunities through communication channels such as the Behind the Buy podcast series, a design approach that allows procurement and program offices to listen and learn about innovative IT contracting strategies. One CIO offered an innovative approach, “[It] would be ideal to have prequalified DevOps firms where I could release Task orders with no protest; goal would be to come up with requirement, procure, and award within one month (\$5-\$10M opportunities).”

There is a profound interest among CIOs and CISOs in redefining the integration of acquisition activities, processes, and information/data to drive results earlier in the development lifecycle, generate cost savings, and improve supplier relationships. To achieve this goal, agencies will need to use existing flexibilities in the FAR and develop better ways to eval-

“We’re investing more in vendor management - In the next few years, Standard Operating Procedures will exist and the information within it will be identical to how Contracting Officer’s Representatives (CORs)/Task Order Managers (TOMs) do business.”




uate contractor performance in a fast-paced environment with rapidly changing requirements. Recently released tools such as the TechFAR Handbook provide additional guidance to agencies on best practices and a compilation of FAR provisions that are relevant to agile development. Another priority effort is the adoption of category management – a new, strategic approach that will enable the federal government to buy smarter and act


more like a single enterprise by identifying core categories of spend, sharing best practices, and providing more streamlined solutions. The goal of category management will be to provide a more transparent federal procurement process by empowering agencies with centralized spending data and contract intelligence to enable them to make more informed purchases that better respond to an agency's needs while leveraging budget resources and benefiting taxpayers.

"Acquisition is a team sport but instead it is handed off between the program Office, Contracting Officer, COTR, and General Counsel. When the requirements are being defined, all of these parties should be working together."

"Make it faster. It doesn't have to be difficult. Believe in bringing in new, innovative organizations. Should not need a contract with an existing company to get in the door. Process is 4-6 months"

Pain Points in *IT Acquisition*

 Education	 Rules	 Process
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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

 Acquisition Changes CIOs Suggest

<ul style="list-style-type: none"> • Improve handoffs and limit surprises through use of integrated teams throughout procurement process: legal, procurement, program, CIO, CFO • Create IT procurement community of practice focused on educating procurement and legal in IT buying best practices – critical this is open to all CO's and Legal staff • Change mindset of procurement and legal to foster more flexible and creative interpretation of FAR 	<ul style="list-style-type: none"> • Increase simplified acquisition threshold • Stop use of LPTA for services contracts • Allow cross agency sharing of contracts • Improve education of IT staff in procurement, assign liaison to procurement • More education on when agencies can and cannot speak with contractors – mythbusters 2.0 – It's OK to meet with industry to discuss RFI and sources sought responses 	<ul style="list-style-type: none"> • Vehicles with longer terms, less protests, more vendor incentives and disincentives • Better align procurement and budgeting process • Better performance metrics, (e.g. requirements repository so agencies can see what has and hasn't worked in the past and what it typically cost)
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



What about the use of LPTA?

"When we have to recompet a contract, we are often forced to use lower cost providers and get C players when they really want to hold on to the A and B players that they are working with and are for whom they are willing to pay a premium. Be more concerned about getting the right result – time to get things done as an example. Cost is weighted too highly and value is about more than that."

LPTA is too common, resulting in poor services. Contracts often end up being recompeted before fully exercised so cost savings from contract change to LPTA provider are lost when cost of acquisition is added back in. LPTA doesn't have a place for service contracts. Some Agencies reported 100% of hardware/software contracts are LPTA and as many as 60% for services. Others that are best value are actually evaluated more like LPTA where Procurement staff are not doing true best value trade offs. "LPTA ends up costing more money in the long run (for a less talented team)."

IT SHARED SERVICES

An overwhelming majority of CIOs and CISOs we interviewed stated they are currently using or plan to implement some form of shared services, with the majority focused on support activities. Key service areas identified by respondents included human resources, time and attendance, case management, financial management, acquisition, administrative, software licensing, email, data center hosting, analytics, cloud and application hosting. Some respondents indicated that, per OMB's mandate, their agency's financial management systems may move to a federal shared service provider. One respondent expressed concern as they noted that "federal shared service providers' budgets are difficult to understand, as they are not structured like businesses, nor are they similar to traditional IT budgets."

Three shared services models primarily used by our respondents included interagency, intra-agency, and commercially outsourced services. One respondent said that they have become a shared service provider within their own department, allowing others to utilize their IT commodity contracts.

Interviewees shared multiple best practices related to this area, emphasizing that there is no substitute for adequate upfront planning and risk assessments. They also indicated that throughout the process, the teams must remain customer-focused, ensuring that changes made will provide customers with the services they need. A strong, well-documented governance structure was also identified as a best practice, allowing decision makers to be involved in key decisions that will impact customers. Finally, strong Service Level Agreements were identified as an essential component. "While these may be more useful when dealing with private vendors," stated one CIO, "there needs to be a clear understanding of the services provided."

CURRENTLY USING OR PLANNING TO IMPLEMENT SHARED SERVICE



- Implementation should be focused on requirements, not politics
- Involve end-users early and often, and make it so that they are bought into the use of shared services
- Gain buy-in across all business functions and understand there will be changes
- Strong people and communication skills are necessary
- Ensure significant planning time is built in upfront to address any business process changes, and any impact on staff (which may require involvement of unions and Human Resources)

WORKFORCE


According to the President's Council on Jobs and Competitiveness, "In the 21st century global marketplace, a nation's economy can only be as strong as the skills of its people."⁷ With budget cuts, hiring freezes, and Baby Boomer retirement, agencies must adopt new approaches to recruit, maintain, and develop a workforce of highly skilled employees.

Recruitment and retention efforts are critical to promoting engagement with younger potential and current members of the federal workforce. While nearly 25 percent of the U.S. workforce is under the age of 30, this demographic composes only 10 percent of the federal workforce. **CIOs hope that by adopting newer technologies this will help attract fresh, forward-thinking candidates who can begin specializing in areas such as: applications, infrastructure, cybersecurity, systems engineering, and project management.** Agencies have begun adopting new strategies to attract the millennial demographic by launching mobile career apps that notify users of job openings, accepting online applications, and adopting the Pathways program.

While USAJobs continues to be the centralized job opportunity location for the federal government, agencies must continue to expand awareness through advertisements at job fairs, social media platforms such as Twitter, and websites that specialize in connecting entry-level employees to employers. To improve retention of current employees, leadership needs to understand what drives employee satisfaction and to build those incentives into the work environment and culture. Agencies have begun providing regular feedback to further reinforce employees' sense of purpose, as well as boosting moral through nonmonetary incentives such as developmental assignments, agency awards, and even thank-you letters from leadership.

⁷ President's Council on Jobs and Competitiveness. "Taking Action, Building Confidence – Interim Report." http://files.jobs-council.com/jobscouncil/files/2011/10/Jobscouncil_InterimReport_Oct11.pdf.

A mission-ready, productive workforce also requires improved training and development opportunities. With constrained budgets, the majority of agencies face added pressure to hire from within, forcing employees to handle increased workloads and unfamiliar tasks. **Sixty-three percent of respondents stated their agencies were “not at all” to “insufficiently” equipped to support their talent development needs.** Some respondents noted employees do not take advantage of training, thereby contributing to the federal skills gap. To promote cost-effective training through cross-agency collaboration, the Department of State successfully implemented an inter-departmental mentorship program. This effort has provided employees with exposure to a broader range of experiences, which is also evident in their recent proposal to provide intra- and inter-departmental rotations and sabbaticals from federal service.



Top workforce Challenges


- An effective plan to facilitate knowledge transfer and retention from current to new workforce

- Leaders skilled in managing and engaging a diverse, mobile, and agile workforce

- The ability to proactively identify emerging trends and challenges and the ability to integrate changes in budgets and operations

- Shift in focus from providing service to delivering value to customers


WORKFORCE



Best Practices

- Improved workforce capacity planning
- Strengthening IT training and certification programs
- Industry/government rotations
- Improvements in recruiting tools and methods
- Flexible work arrangements

Biggest Skills Gaps



- Technical knowledge: cyber, cloud, mobility
- Leadership
- Strategic planning
- Agile service delivery
- Business acumen

“Training is one of the first things to go with budget cuts. The need to keep employees current on technology is currently non-existent. When this happens, the agency starts to see morale problems because the employees are overworked and undertrained.”

To fully capitalize on the benefits of investing in workforce engagement and development, the federal government must also invest in succession planning and retiree knowledge sharing. The potential knowledge gap is evident: GAO predicts that over a third of the federal workforce will be retirement-eligible by September 2017, and 62 percent of retired federal employees said they did not train a new employee before their retirement, according to a Federal News Radio survey.⁸ The federal government has responded by offering mentoring and training opportunities through the rehiring of retirees and President Obama’s Phased Retirement program. Though a step in the right direction, there are constraints on the number of reemployed annuitants, and many agencies have yet to adopt these knowledge-sharing programs. Due to these limitations, additional efforts should include: 1) skill inventory gap reports identifying near-term and long-term hiring needs; 2) more clearly defined job vacancy announcements; 3) automated tools that decrease the hiring process wait times; and 4) building a recruitment pipeline with targeted schools and colleges.



8 O’Connell, Michael. Federal News Radio. 28 April 2015. Accessed 5/31/15. <http://www.federalnewsradio.com/204/3846361/Feds-choose-to-stay-longer-creating-new-retirement-bubble>

WHAT'S TO COME?

Interviewees estimated that currently 39 percent of the federal workforce are federal employees, while 61 percent are contractors. When asked how this will change over the next four years, respondents indicated there will be a decrease in contractor support, on average moving towards a workforce composed of 51 percent federal employees and 49 percent contractors. While these figures only represent estimates provided by interviewees, if more work continues to shift from contractors to federal employees, retention and training initiatives will be critical in mitigating the skills gap and stimulating employee morale. For stronger succession planning, agencies need to engage in comprehensive analysis of workforce demographic and development data to support strategic investment.

“Another challenge we face is retirement. Unfortunately, you can't predict when someone is going to retire. An agency needs to have an orderly transfer of knowledge. If you have a pipeline of talent, you should constantly be growing that talent so that if someone does retire, they can be easily replaced.”

CONCLUSIONS

It's clear from this year's 25th anniversary survey that CIOs and other federal IT executives play a central role in the success of their agencies. CIOs continue to be called on to deliver more innovation, better performance, more return on investment and an enhanced customer experience – all while protecting crucial systems from a rapidly expanding set of threats that continue to morph and become more sophisticated.

Some trends are apparent across government IT from our interviews. Like their private-sector counterparts, mobility – of both the workforce and the information systems – remains a high priority for CIOs, their customers and staff. Applications are rapidly moving to cloud-based models, providing gains in performance and reductions in cost. An overwhelming majority of CIOs and CISOs we interviewed stated they are currently using or plan to implement some form of shared services, with the majority focused on support activities.

In the wake of failed launches of large-scale IT programs, federal IT managers are quickly moving to embrace modular development where failures, if they happen, can be more easily managed. In this Agile-powered environment, agencies are going through a culture change focused on building and delivering quickly, allowing for experimentation and failure, and ultimately faster time to stakeholder satisfaction.

However, several factors impede achievement of the numerous objectives that land in the CIO's ever-expanding inbox. One challenge is the stiff competition for IT talent. Only 10 percent of the federal workforce is under 30 compared to 25 percent of private-sector employees. Another hindrance is the fear of failure hanging over professionals that work in many federal agencies, sometimes stifling the innovation that is expected from IT departments. Finally, agencies continue to face budget uncertainty and limited acquisition resources.

While there are certainly challenges to be surmounted in the federal IT sphere, there are many gains to be celebrated, and even more to look forward to with digital convergence and a mobile-enabled revolution on the horizon. CIOs are poised to become the innovative leaders of a future federal government that is more responsive, nimble and cost-effective than ever before in our nation's history.

APPENDIX A - LIST OF INTERVIEWEES

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

BRIAN ABRAHAMSON
Chief Information Officer
Pacific Northwest National
Laboratory, Department of Energy

DORINE ANDREWS
Chief Information Officer
Peace Corps

DARREN ASH
Chief Information Officer
Nuclear Regulatory Commission

DOUG BAILEY
Deputy Administrator
Information Technology Service
Agricultural Marketing Services
Department of Agriculture

MIKE BARTELL
Chief Information Officer
Oak Ridge National Laboratory
Department of Energy

TOBY BENNETT
Director
Office of Program Administration
Organization, U.S. Patent and
Trademark Office
Department of Commerce

DAVID BRAY
Chief Information Officer
Federal Communications
Commission

LORETTA BURNS
Deputy Chief Information Officer for
Programs, Farm Service Agency
Department of Agriculture

SYLVIA BURNS
Chief Information Officer
Department of the Interior

DAN CHADDOCK
Associate CIO for Enterprise Services
Internal Revenue Service
Department of the Treasury

RICHARD COFFEY
Associate Chief Information Officer
Enterprise Data Center Operations/
National Information Technology
Center, Office of the Chief
Information Officer, Department of
Agriculture

KATHY CONRAD
Principal Deputy Associate
Administrator, Office of Citizen
Services and Innovative
Technologies
General Services Administration

KEVIN COOKE, JR.
Deputy Chief Information Officer
Department of Housing and Urban
Development

SCOTT CORY
Chief Information Officer/Director of
Resources Management
Administration for Community
Living

THERESA CULLEN
Chief Medical Information Officer
Veterans Health Administration

MARK DAY
Deputy Assistant Commissioner
Integrated Technology Service
Federal Acquisition Service
General Services Administration

KEVIN DEELEY
Deputy Chief Information Officer
Department of Justice

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

MIKEY DICKERSON
Administrator
U.S. Digital Service

MARTI ECKERT
Associate Commissioner
Office of Information Security
Social Security Administration

LESLEY FIELD
Deputy Administrator
Office of Federal Procurement Policy
Office of Management and Budget
Executive Office of the President

MARTY FINKELSTEIN
Deputy Chief Financial Officer
Immigration and Customs
Enforcement, Department of
Homeland Security

JAMES FLANAGAN
Deputy Chief Information Officer/
Director, Office of Information
Services, Nuclear Regulatory
Commission

PETER FONASH
Chief Technology Officer
Cybersecurity and Communications
Department of Homeland Security

ROBERT FOSTER
Deputy Chief Information Officer
Department of Health and Human
Services

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

LARRY GROSS
Principal Deputy Chief Information
Officer, Department of the Interior

RICHARD HALE
Deputy Chief Information Officer
for Cybersecurity, Department of
Defense

DEAN HALL
Associate Executive Assistant
Director/Deputy CIO, Information
and Technology Branch
Federal Bureau of Investigation
Department of Justice

SONNY HASHMI
Chief Information Officer
General Services Administration

RICK HOLGATE
Assistant Director/Chief Information
Officer, Bureau of Alcohol, Tobacco,
Firearms & Explosives, Department
of Justice

JOYCE HUNTER
Acting Chief Information Officer/
Deputy CIO, Policy and Planning
Office of the Chief Information
Officer, Department of Agriculture

STAN KACZMARCZYK
Acting Director of Strategic
Programs, Office of Integrated
Technology Services, Federal
Acquisition Service
General Services Administration

NICOLE KERKENBUSH
Military Deputy Program Executive
Officer, Defense Healthcare
Management Systems

JOSEPH KLIMAVICZ
Chief Information Officer
Department of Justice

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

JEFF KOSES
Senior Procurement Executive
General Services Administration

JONATHAN KRADEN
Senior Counsel, Homeland
Security and Governmental Affairs
Committee, United States Senate

WILLIAM LAY
Deputy CIO for Information
Assurance/Chief Information
Security Officer, Bureau of
Information Resource Management
Under Secretary for Management
Department of State

DAWN LEAF
Chief Information Officer
Department of Labor

ROBERT LEAHY
Associate CIO for Strategy and
Planning, Internal Revenue Service
Department of the Treasury

RUSSELL LEWIS
Associate Chief Information Officer
Internal Revenue Service
Department of the Treasury

GEORGE LINARES
Chief Technology Officer
Office of Information Services
Centers for Medicare & Medicaid
Services, Department of Health and
Human Services

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

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

ALAN MCCLELLAND
Information Security Specialist
Food and Drug Administration,
Department of Health and
Human Services

DENNIS MCCRARY
Deputy Chief Information Officer
Drug Enforcement Administration
Department of Justice

RICHARD MCKINNEY
Chief Information Officer
Department of Transportation

ANDREA NORRIS
Chief Information Officer
National Institute of Health
Department of Health and
Human Services

DREW ORNDORFF
Associate CIO and Chief Information
Security Officer, Office of the
Chief Information Officer,
Department of Transportation

JOHN PARDUN
Cybersecurity Division Director
U.S. Patent and Trademark Office
Department of Commerce

STACY RIGGS
Acting Director
Office of Enterprise Planning and
Governance, Office of Information
Technology, General Services
Administration

ANNE RUNG
Administrator, Office of Federal
Procurement Policy, Office of
Management and Budget
Executive Office of the President

LISA SCHLOSSER
Deputy Administrator, Office of
E-Government and Information
Technology, Office of Management
and Budget, Executive Office of
the President

RORY SCHULTZ
Deputy Chief Information Officer
Food and Nutrition Service
Department of Agriculture

MARK SCHWARTZ
Chief Information Officer
Citizenship and Immigration
Services, Department of
Homeland Security

JEFF SEATON
Chief Information Officer
Langley Research Center
National Aeronautics and Space
Administration

CHAD SHERIDAN
Chief Information Officer
Risk Management Agency
Department of Agriculture

NANCY SIEGER
Associate Chief Information Officer
Internal Revenue Service
Department of the Treasury

HARRY SINGH
Deputy Associate Director/Chief
Information Officer, Bureau of
Engraving and Printing
Department of the Treasury

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

RONALD THOMPSON
Executive Director of IT Operations
Department of Health and
Human Services

KEITH VANDERBRINK
Director, Financial Resources
Management Division, U.S. Patent
and Trademark Office, Department
of Commerce

GARY WASHINGTON
Chief Information Officer
Natural Resources Conservation
Service, Department of Agriculture

BARRY WEST
Chief Information Officer
Federal Deposit Insurance
Corporation

RENEE WYNN
Deputy Chief Information Officer
Environmental Protection Agency

KEVIN YOEUL PAGE
Deputy Commissioner
Federal Acquisition Service
General Services Administration

APPENDIX B - LIST OF INTERVIEWERS

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

PSC

DAVID M. WENNERGREN
DONALD BAUMGART
GRANT THORNTON
SURVEY TEAM

GEORGE DELPRETE

SAIRAH IJAZ

STEPHANIE GEORGE
CIO SURVEY
INTERVIEWERS

CYNDI AGLORO
Grant Thornton

MASHAAL ALI
Grant Thornton

LEE ANN ANDERSON
Unisys

MELANIE ANGE
Centurylink

MEREDITH BARNARD
Grant Thornton

CAL BASSFORD
Grant Thornton

AARON BEASON
Grant Thornton

ADRIANNE BERMAN
Grant Thornton

AURPON BHATTACHARYA
Grant Thornton

CINDY BISHOP
SRA International

DANIEL BLUM
Grant Thornton

MICHAEL BORDEN
General Dynamics

MICHAEL BRUCE
BAE Systems

ROB BUHRMAN
Grant Thornton

ANGELA BUTLER
Vistrionix

DIANA CEBAN
OST, Inc

NILESH CHUDASAMA
Grant Thornton

EMILY CACCIO
AT&T Government Solutions

TOM COCOZZA
Grant Thornton

BILL COHEN
Sutherland Global

SUE CONTOSTAVLOS
IT Cadre

JENSON DANIEL
Organon Advisors

GEORGE DELPRETE
Grant Thornton

AVINASH (AVI) DEOLALIKAR
AT&T Government Solutions

GIOVANNINA DIPIETRO
General Dynamics

ED DUBOIS
NetApp

AMY FADIDA
A.M. Fadida Consulting

SHEILA FARLEY
Centurylink

MATT FILIZOLA
Red Hat, Inc.

ERIC FORSETER
NetIQ

MARIA GABOURY
Harris Corporations

STEPHANIE GEORGE
Grant Thornton

LANCE GLOGOVAC
Century Link

ROBERT HAAS
Hewlett Packard

ERIC HEFFERNAN
Grant Thornton

CHRISTIAN HOEHNER
Van Scoyoc Associates

BRAD HUNTER
Grant Thornton

SAIRAH IJAZ
Grant Thornton

ANNE IMRIE
General Dynamics

ROB IRISH
Grant Thornton

VIPIN JAIN
Hewlett Packard

CHUCK JAMES
Hewlett Packard

JOHN KENNEDY
Centurylink

TORI KEY
Grant Thornton

ZHENIA KLEVITSKY
PricewaterhouseCoopers

JOHN KONCZYK
Grant Thornton

CHRISTINE KRAFT
AT&T Government Solutions

TIM LAWLER
Grant Thornton

ALVIN LEWIS
CenturyLink

KRISTEN LILLARD
Grant Thornton

ANDY LUCIDO
Grant Thornton

GEOFF LUIZ
Grant Thornton

LIZ LYDON
IT Cadre

BOB MAHONEY
Harris IT Services

BRAD MARCHAND
Grant Thornton

DAVID MARTIN
Teradata

FELIX MARTINEZ
Deloitte

DAVE MCGINN
Hewlett Packard

SHIRLEY MENISH
Harris Corporation

KATHY MINCHEW
Federal Insights, LLC

DEIRDRE MURRAY
CenturyLink

ISAAC NEGUSSE
AT&T Government Solutions

KEN NEWCOMER
ICF International

JIMMY NORRIS
Grant Thornton

JIM O'NEILL
Red Hat, Inc.

DAVE PEARL
Grant Thornton

TONYA POWERS
Accenture

F. CRAIG REICHENBACH
Brocade

RON RHODES
OST Inc.

PHYLLIS RIENZO
NetApp, Inc

VINCENT ROBERTS
Grant Thornton

DAN ROGERS
Grant Thornton

RANDY ROSE
PricewaterhouseCoopers

ERIC RUSSELL
CenturyLink

PAT SAVOY
Grant Thornton

DAVID SAXE
Techflow

JAMES SCAMPAVIA
AMERICAN SYSTEMS

MARY JEAN SCHMITT
NetApp, Inc.

JON SHALLANT
Red Hat, Inc.

BRENT SHOEMAKER
Level3

CLIFF SINK
Hewlett Packard Enterprise Services

PETE SNYDER
Level3

LORI STALLARD
Lockheed Martin

SIMON SZYKMAN
Attain

WEI TANG
Grant Thornton

CLARENCE TAYLOR
NJVC

DAN TWOMEY
Twomey & Associates

ROBERT TURNER
Xerox

SONJA TWIFORD
Grant Thornton

GREG WALLIG
Grant Thornton

ANTOINETTE WILLIAMS
Williams Consulting, LLC

BEN WILSON
Grant Thornton

BRIAN YAKIMOWICZ
NetApp, Inc.

MATTHEW ZIRPOLI
Harris IT Services

AKNOWLEDGEMENTS

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, 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

Senior Vice President, Technology

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, Information Technology

ABOUT THE SPONSORS

PROFESSIONAL SERVICES COUNCIL (PSC)

The Professional Services Council (PSC) is the voice of the government technology and professional services industry, representing the full range and diversity of the government services sector. 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 370 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 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.



PROFESSIONAL SERVICES COUNCIL

4401 Wilson Blvd #1110
Arlington, VA 22203
(703) 875-8059
www.pscouncil.org



**GRANT THORNTON LLP
GLOBAL PUBLIC SECTOR**

333 John Carlyle Street, Suite 400
Alexandria, VA 22314
703.837.4400
www.GrantThornton.com/publicsector