PSC
PROFESSIONAL
SERVICES
COUNCIL

GrantThornton

TRANSITIONS
Managing Federal IT in a Dynamic Environment

Contents

About The Survey

This survey is sponsored and led by the Professional Services Council (PSC) and PSC-member company Grant Thornton. Grant Thornton has surveyed federal Chief Information Officers (CIOs) for 27 years. In recent years, the survey has expanded to include additional senior information technology (IT) officials, including Chief Information Security Officers (CISOs) and Chief Data Officers (CDOs) as well. This year we expanded our survey again to include an online survey of agency IT personnel.

Through these surveys, top IT officials, agency IT personnel, oversight groups, and Congressional staff shared their views on challenges facing federal CIOs and the federal IT community. As in past years, we received outstanding support from the federal IT community in conducting this survey.

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

Interviews conducted
APRIL 2017 – JULY 2017

CISOs
Information Technology Specialist
Information System Program Manager
Security Controls Director CDOs CIOs
Analyst CTOs IT Administrator
PMO Analyst Senior Information Security
Specialist Account Technician

313
Respondents

YEARS IN ROLE
65% 0-3 years   29% 4-7 years   6% more than 7 years

IN PERSON   **ONLINE**

17 Agencies participated

29 Agencies participated

YEARS IN ROLE
23% 0-3 years   17% 4-7 years   60% more than 7 years

23 CIOs, CISOs, and other IT officials

78% Federal Employee   **7%** Contractor   **15%** Other*

*(ie State Employee, Non-Profit, County)

Executive Summary

The federal IT community has seen a tremendous amount of change in 2017. The transition to a new presidential administration has brought with it opportunities and challenges for agency IT leaders. Among the Trump Administration's priorities are bringing more innovation into government and modernizing federal IT to better serve Americans. This shines a spotlight on the role of Chief Information Officers (CIOs).

Putting in place new agency leadership, including many CIO and senior level IT positions, however, has been slower than usual. As of September 2017, nominees have yet to be named for the federal CIO, the and newly-created federal Chief Information Security Officer (CISO) position at the Office of Management and Budget (OMB) and 13 of 27 CIO positions at the largest federal agencies remain open. This leaves agencies without guidance and input from politically-appointed leaders into many existing IT initiatives and hampers efforts to fully develop new projects and investments. At the same time, IT acquisition and management remains a focus of Congressional hearings and oversight efforts.

Despite these additional challenges, IT leaders have continued to push forward, trying to do more, do it better, and do it with less money. Over the last year, the federal IT community has striven to balance oversight of operations for mission critical functions with opportunities to bring innovative services and efficiencies into government, all while building more effective cyber defenses as the threats to government systems continue to increase. And all of this work is happening in an uncertain budget environment where agencies often lack access to resources and high-level support to meet all the demands.

While CIOs, CISOs, and other senior IT leaders in government continue to coalesce around a similar set of priorities in 2017, rank and file government employees are not always receiving clear messages about what those priorities are. The addition of an online survey to our reporting process this year revealed a lack of consistency between priorities identified by senior IT leaders and other federal IT employees. For example 75 percent of CIOs identified DevOps as a top priority compared to only 28 percent of online respondents. When asked about the use of Agile, 80 percent of online respondents said Agile was used on less than half of IT projects while 57 percent of CIOs responded that Agile is used on more than half. This could be due to the presidential transition and lack of guidance from the new administration. CIOs and other IT leaders should nevertheless ensure everyone in their organization and across their agency has access to and is familiar with the most important priorities and goals.

At a time when leveraging innovation to meet agency goals is more important than ever, federal IT leaders can play a driving role in improving efficiency and performance across government.

Top Priorities and Challenges in IT

Each year, we ask CIOs an open-ended question to uncover the top priorities and challenges they are currently facing. In order to gain a broader perspective this year, we extended this question to a wide range of government employees from across the federal government.

Perhaps the most interesting finding from this expanded audience is the divergence of answers we received from the two different audiences.

For agency CIOs and senior leadership, the top priorities and challenges were very consistent both across their peers and with survey responses from prior years. IT leadership cited cybersecurity, IT modernization, people and culture, cloud, and lack of resources as top priorities and challenges.

Our online survey respondents were in alignment with IT leadership in some of these areas, ranking cybersecurity, IT modernization, and lack of resources at the top of their lists. But very few online survey respondents put people and culture or cloud among their top picks.

This survey report explores many of the top priorities and challenges identified in our research in 2017 as well as the highlights and innovation IT leaders are most excited about.

Cybersecurity

As in past years, cybersecurity remains the top priority identified by CIOs in the 2017 survey. Our survey polled leaders from across the federal government to gain insight into the trends, threats, technologies, and best practices shaping their cyber risk and readiness posture. Federal CIOs believe insider threat, training / workforce developments, and phishing are the three greatest cyber threats. However, when the federal IT workforce was asked how effective their cybersecurity posture was, most respondents replied "unsure." These are the people on the "front lines" for their agencies' security and they are not entirely knowledgeable about the IT security posture of their organizations.

The table below shows the overall ranking of cyber threats when assessed across the population.

What are the biggest threats and challenges your organization faces in cybersecurity? Rank your top 7 in order.

| Item	Overall Rank	Rank Distribution	Score	No. of Rankings
Vulnerabilities from aging applications and technologies	1		216	44
Human error	2		174	37
Malware	3		168	41
Phishing campaigns	4		165	41
Internet-facing attacks (including DDOS attacks)	5		137	37
Insider threat	6		136	35
Cybercrime	7		123	37
Ransomware	8		77	20
Supply chain technology security	9		75	23
Other	10		7	3

Lowest Rank   Highest Rank

So how are government IT leaders working to make sure the IT workforce is aware of these new threats? Both CIOs and the federal workforce see cybersecurity awareness being raised via online trainings and emails and other creative education tools. One agency has a cyber tip of the day that must be answered before employees can log into their computers. Another holds monthly cyber campaigns around various topics – they described a spearfishing campaign designed to trick employees. They sent fake emails to 95,000 staff and ten percent opened them. Those who opened the note received a message informing them they had failed the test and received additional education training. Despite these efforts, there is still room for improvement, with 52 percent of survey respondents and 38 percent of CIOs calling these methods only "somewhat effective." Dynamic security awareness practices such as phishing, vishing, and hacking campaigns can have a much more powerful impact on an organization than an online training or slide show might have according to survey respondents. Some organizations are using specialized phishing software that creates realistic spoof emails to test their users' response and awareness in real time.

The one thing that is clear from our survey results is cybersecurity threats are on the rise. Thirty-four percent of our respondents reported a rising trend in cybersecurity threats while only three percent reported a decrease. One CIO said they had received 100M attacks in one day through WordPress and typically received 1M attacks per day. The threats through social media sites like Facebook and Twitter are growing as well.

Have you seen an increase or decrease in cyber threats? Or have they stayed the same?

35% Increase

3% Decrease

31% Stay the same

31% Unsure
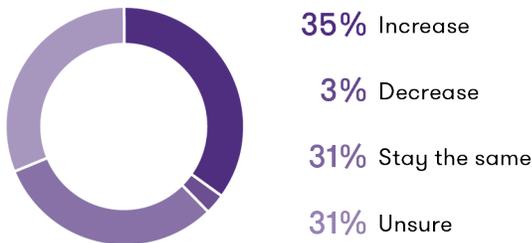
One CIO stated:

"There is a constant battle with cybersecurity. The agency is playing catch up and looking at different tools to invest in for monitoring and patching to quickly remediate vulnerabilities."

One CIO said it is becoming expensive to get the right tools. "New tools are only good for six months because everything changes so quickly and the budget process doesn't support this. This is a big threat." Another stated, "we need better tools and analytics," explaining the volume of cyber data being collected

is overwhelming. Another CIO expressed the need "for more machine learning to root out false positives because the volume of cyber data collected was growing exponentially and extremely difficult to analyze."

On a positive note, respondents reported an overall improvement in their cyber posture from the previous year, with 47 percent of the respondents agreeing with the statement, "My agency is more effective at identifying and mitigating cyber risks today than we were a year ago," versus only 13 percent who disagreed.

CIOs ranked vulnerabilities from aging technology and human error as the biggest challenges to their overall cybersecurity. With regards to aging technology, federal legacy IT investments are becoming increasingly obsolete. Many use outdated software languages and hardware parts that are unsupported. Agencies reported using several systems that have components that are, in some cases, at least 50 years old.

CIOs also expressed the continuing challenge of trying to recruit and retain qualified cybersecurity personnel. One CIO referred to "a very slow hiring process, and a security budget that was too small to attract and retain qualified cyber staff." Another CIO cited that even though they had a special hiring authority that allowed them to "pay a 25 percent pay bump for cyber staff, it isn't high enough – it only gets 2nd and 3rd tier cyber talent, not the A team." Another stated, "we lack the cyber workforce because pay isn't equitable with the private sector," and suggested they develop a cyber pay scale between GS15 and SES rates to attract top cyber talent. Some CIOs did express that the federal cybersecurity workforce strategy developed in 2016 was positive as well as the OPM cyber careers website (www. cybercareers.gov) launched in January 2017 and collaboration around hiring fairs for various agencies.

"It's very difficult to recruit and acquire cyber talent. Agencies are really competing against each other for the same talent."

Funding IT Modernization

IT modernization has remained at the top of senior IT leaders' priorities lists in 2017 with 72 percent of CIOs responding over half of their applications are legacy systems. Further proof is that a significant portion of the federal IT budget continues to be spent on Operations & Maintenance while funding for Development, Modernization, and Enhancements (DME) has decreased by more than six percent from FY16 to FY17, according to the IT Dashboard (www.itdashboard.gov).

What percentage of your agency's IT budget will be allocated to modernizing your legacy applications?

21% 0% - 20%

11% 21% - 50%

5% 51% - 75%

6% 76% or more

57% Unknown

0   10   20   30   40   50   60
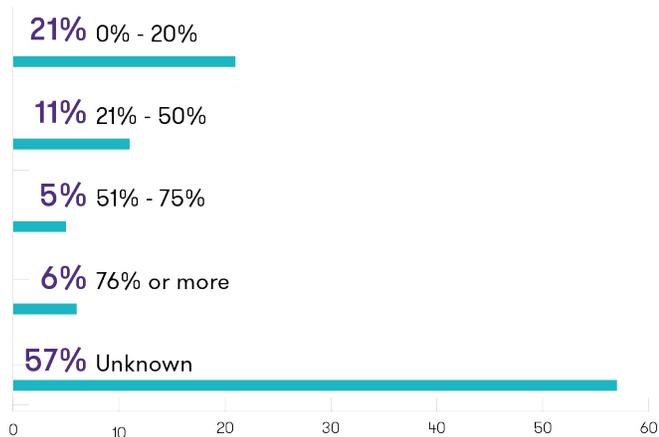
The American Technology Council's August 2017 draft report on federal IT modernization outlines a vision for federal IT focused on enabling more rapid delivery of new capabilities to the American people, increased cybersecurity, and more cost-effective management. The report cites a number of barriers to modernization ranging from procurement challenges to outdated policy and technical guidance. CIOs generally agreed with these findings and cited similar challenges.

While many CIOs have been able to make incremental progress in modernizing some systems, there is still not sufficient funding to get ahead of the curve. One CIO said, "Currently we face challenges of fighting for funding and streamlining communication between all of our field offices." Agency IT staff responses also emphasized this reality and even expressed concern that "technology is surpassing us" as they wait to upgrade outdated systems. One noted the average age of their IT staff is 48-50 years old, and they do not know the latest computer languages and platforms needed to take advantage of available modernization options.

> "A conservative estimate has our government's technology spending at over $80 billion dollars a year. Annually, over two-thirds of these costs are spent maintaining legacy systems. This structure is unsustainable."[1]
>
> **–White House Senior Advisor Jared Kushner[1]**

This sentiment that funding for IT investments has not kept up with the pace of innovation was consistent across all respondents this year. Some pointed out the approach of even distribution of funding when it comes to IT modernization is counterproductive. As one respondent stated, "the piecemeal approach to funding IT projects hampers most, if not all, federal agencies."

That reality made the release of the President's budget request for FY18 all the more stark. Although the budget seeks an overall increase in funding, the request represents just a 1.7 percent increase, slightly below the historic average growth in spending. In fact, across all the top challenges CIOs and IT staff shared this year, the lack of resource is always at or near the top.

Continued underfunding complicates agencies' IT modernizations efforts. Yet many are optimistic about legislative efforts–especially the Modernizing Government Technology Act (MGT),[2] and the Trump Administration's budget request to create larger and more flexible working capital funds for IT investments.

There are IT leaders who are content with some of their legacy systems remaining, citing the decreased risk to hacking as a rationale. One CIO stated, "Legacy doesn't mean it's a bad system. If it is working and meeting the business requirements, it's fine [and] lets you sleep at night. Many legacy systems are more secure than those running on modern platforms. You don't hear about mainframes getting viruses."

One important lesson learned in IT modernization is that the decommissioning of a legacy system is a whole project in itself. Many agencies just keep on operating the legacy hardware and software and do not go through the rigor to formally deactivate, dismantle and retire old systems. According to one respondent, "there should be a federal award program to recognize teams when they actually pull the plug to decommission legacy systems." CIOs are up to the challenge though. One CIO has issued a prohibition for development of legacy systems, which has helped to reduce O&M spending. Another CIO has moved from 200 to 30 legacy applications and is moving to a fully outsourced network as a service.

Federal IT Spending (in millions)[3]

$ Millions

Year	FY13	FY14	FY15	FY16	FY17	FY18
Total	77,897	81,810	86,692	88,712	89,850	95,588
Non-Defense	41,273	44,396	49,965	50,726	51,300	53,167
Defense	36,624	37,415	36,727	37,987	38,551	42,521

■ Defense ■ Non-Defense ■ Total
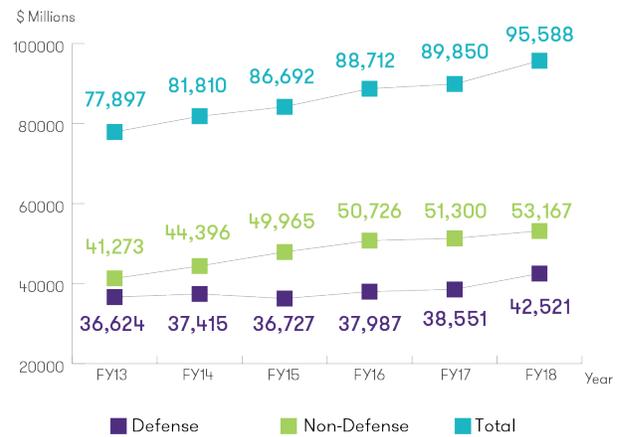
2 H.R. 2227 / S.990 [115th Congress].

3 Analytical Perspectives, Budget of the U.S. Government, Fiscal Year 2018.
   https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/spec.pdf.

People and Culture

It is very difficult to accomplish goals without the right people on the job. Some of the progress government agencies have made recently was stalled over the first six months of the Trump Administration with a hiring freeze and continued budget uncertainty. For senior IT leaders, this is a significant roadblock in making progress on IT initiatives. One CIO said the "federal government needs to bring the right talent to the table... none of this happens without the right people."

The CIOs are not the only ones feeling the impact of an under-resourced and skilled staff. One in four online respondents believe the lack of resources has a significant negative impact on staff morale and leads to staff burnout. "We are facing a workforce problem as workers are overworked and underpaid." Shifting resources to tasks they are not qualified to do may result in significant rework and missed targets on CIO initiatives.

> "We'd love to acquire more people with scientific skills to support security analytics. But because of salary caps, we have a difficult time attaining the top talent."

Lack of funding also makes finding and investing in new talent very difficult. One CIO noted federal employees may not be able to advance in their career at one agency and, after reaching the top of their organization, get picked up at a higher pay grade at another agency.

FITARA, TBM, and the Role of the CIO
Enacted in 2014, the Federal IT Acquisition Reform Act (FITARA) aimed to enhance the role of agency CIOs and improve how government purchases IT. The 2017 FITARA Scorecard gave only one of 24 covered agencies an "A" grade on implementing this law.[4] Many CIOs surveyed this year reported minimal impact from FITARA, or incomplete progress to fully realizing the law's goals. One noted while CIOs now have more direct control of much of their agency's IT spending, they still do not oversee

significant amounts of "shadow" IT purchases by agency divisions or offices. Another CIO said it would take $25M to effectively implement FITARA in his agency and they just do not have that money.

Technology Business Management (TBM) is a business model and decision-making framework for maximizing the business value of IT. A few CIOs discussed how TBM, which creates a standardized IT costing taxonomy, could facilitate implementation of FITARA. The Office of Management and Budget (OMB) through Circular A-11 and changes to the capital planning and investment control process has asked agencies to break out their spending on IT in more depth in the FY19 budget process. One CIO shared they see agency approaches to TBM in 3 groups: a handful of leaders who are fully invested, the majority who are examining it and just getting started, and a 3rd group who are taking a "wait and see" approach. CIOs who have fully jumped into implementing the TBM framework are investing in software and IT cost reviews and have a much clearer understanding of duplicative enterprise IT spending. One CIO in the middle group recently asked his innovation office to explore how it could be applied. Another CIO felt it would be very difficult to implement TBM because of the way in which financial systems capture IT cost information, and making changes in those systems is overly expensive. One CIO who is taking a wait and see approach thinks the service catalog and cost tracking against it offer the same transparency with much less investment. All CIOs did believe that a framework like TBM has utility in helping to achieve FITARA.

CIO Authority Enhancements under FITARA
FITARA increased the authority of agency CIOs over IT spending. This law requires CIOs at 24 of the largest federal agencies to:
- Approve agencies' IT budget requests;
- Review and approve IT contracts; and
- Certify that IT investments are following incremental development guidelines.

4 U.S. House Committee on Oversight and Government Reform. https://oversight.house.gov/wpcontent/uploads/2017/06/FITARA.

Top Innovations

CIOs and other IT leaders are continuously striving to innovate within their agency while balancing the operational demands to "keep the lights on," work within skinny budgets, fulfill ongoing–and often unclearly defined–requests from governing entities. Despite the roadblocks and red tape that can quickly derail new ways of achieving IT goals, senior IT leaders have been able to deliver and build on the success of their IT innovations created in-house or adopted and tailored.

Participants in our 2017 survey cited three areas of innovation and change they were most excited about: adoption of Agile practices, creation of DevOps processes, structure, and culture, and continued progress moving relevant systems and services to cloud computing platforms.

What innovations and accomplishments are you most excited about?

"Moving a whole agency–not just a single component–to the cloud."

"Many of our workers are embracing Agile and we have a number of advocates for our shared services."

Agile

2017 marks another year of increased adoption of Agile practices, according to federal CIOs and senior IT leaders, with some agencies adopting Agile as the standard across the entire organization. When asked what percentage of their IT development projects are utilizing Agile, 56 percent of CIOs stated more than half of their applications are developed using Agile approaches, compared to last year, where 26 percent of CIOs stated Agile was the default.

Senior IT leaders shared their excitement about increasing the use of Agile. One agency CIO was excited to have finally broken through resistance from IT staff who do not have experience outside of the traditional waterfall practice, "It's still a challenge, but we have seen improvements in shifting our culture. Many of our workers are embracing Agile."

Top 3 benefits of Agile

| Better management of change priorities | Increased software quality | Faster time to delivery |

When asked how their agencies share and educate personnel on Agile best practices, online survey respondents reported a variety of ways, with the three most common being in-house training, learning on the job, and working with contractors. Fewer respondents indicated their agencies were leaning on collaboration with other agencies and certifications/external training to get the requisite Agile knowledge and skills.

Some CIOs continue to note a few of the same challenges implementing Agile for large IT development projects from last year, but overall, there was a notable shift to CIOs reporting issues indicative of their agencies' increasingly mature Agile processes. The agencies that are over the hurdle of initial Agile adoption are reporting issues with non-development related activities. For example, one respondent said, "[One] challenge, not limited to Agile, [is that] development [and] test environments do not allow for full scale testing." Another respondent noted other challenges to adopting Agile practices include difficulty with customer buy-in during development the process and weak points in load testing and performance. Our survey saw responses related to not having enough skilled Agile practitioners and trouble getting some groups on board with Agile, with a drop in responses related to procurement related issues. This reinforces the point that, as more agencies adopt Agile as the default, challenges begin to occur in other areas of the organization that are not used to the new speed of development.

Another challenge reported in last year's survey was ineffective use of metric and performance analysis. In 2016, when asked how their agencies measure the effectiveness of Agile delivery, CIOs reported a number of different ways. While there is no true "one size fits all," there are consistent trends among those reported in the 2017 survey. One CIO said, "We measure the effectiveness [of our Agile projects] through the use of the Earned Value Management process and we use it to identify investments that can be a risk." Another CIO stated, "We don't have a formula, but look at on-time delivery and customer/management satisfaction. We need to make sure that it is the customer who defines what completion is."

Other ways in which CIOs measure the effectiveness of Agile delivery include customer satisfaction, user defect rate, number of times they reiterate in cycles, user acceptance testing (UAT) defect findings, use case growth, time to production, use case delivery velocity, time point analysis, planned versus actual sprint success, and burndown charts.

What percentage of your IT development projects are utilizing Agile methodologies?

39% 0% - 20%

43% 21% - 50%

7% 51% - 75%

11% 76% or more
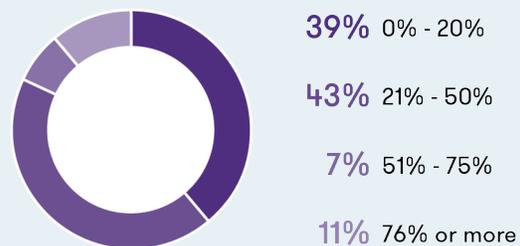
While CIOs are evaluating a variety of metrics to measure Agile, our online survey findings indicate that almost half of respondents feel their agency does not do a good job of measuring the effectiveness of Agile projects.

Overall, CIOs optimistically report their organizations are embracing Agile and seeing benefits. When asked what have the benefits and challenges been as their agency implements Agile, one respondent reported, "[We are] not completing projects faster, but seeing better teamwork, communication and cooperation as well as a better understanding of the entire goal." Another CIO reported, "The feedback loop is much better. The ability to develop a quick prototype to present to the customer allows us to collect feedback information from the customer and make rapid changes in the process based on the feedback."

While the outlook is positive for Agile use in the federal government, there are also lessons to be learned. Some cautionary advice from our CIOs captured during our in-person interviews is that it is important to look at resources, dependencies, and constraints to meet a control; that we must be careful with over-customization of an application to the point that it is rendered useless; and the need to balance cybersecurity and financials alongside Agile development.

We asked online survey respondents what has been the most difficult aspect of implementing Agile. Below is a visualization of their responses

board system acquisition acceptance challenge advance support bugs achieve visualization agile financial area accurate requirements audit difficult availability applicable authorization

Agile Lessons Learned
- Teams may require Agile transition led by an Agile practitioner or coach
- Product owner involvement is imperative to success
- Do not superficially adopt Agile and expect results without commitment
- Focus on building in quality; low defect rates mitigate unplanned work
- Invest in organizational change required to adopt Agile
- Metrics are useful in root cause analysis, but can undermine team dynamics if used improperly
- Deployment pipeline automation reduces operational risk associated with manual deployment and recovery

Agile Best Practices
- Focus on the team, team-based training drives an Agile mindset, develop people to improve performance
- Establish and use definition of "ready" and "done"
- Use iterative planning techniques to incorporate feedback and deliver value
- Deliver small, incremental, potentially shippable, vertical slices of work
- Use metrics to drive achievement of Lean objectives and continuously improve
- Automate your deployment pipeline

DevOps

DevOps is finally breaking into the government space as a culture that is becoming adopted by IT organizations across more and more federal agencies. According to this year's survey, there is a steady increase in the adoption of DevOps that embodies cultural philosophies, practices, and tools that increase an organization's ability to deliver applications and services at high velocity. DevOps popularity has been gaining more slowly than Agile, and 75 percent of CIOs report their organizations are now adopting DevOps.

One of the most common problems found in public sector IT are siloed IT operations and the inability to integrate systems that lead to an over-reliance on manual processes and longer system down times. Federal government organizations are formed around functional silos and have existing processes that require hand-offs and approvals, slowing down development and increasing error rates.

Benefits of DevOps realized by CIOs and their organizations include:

More frequent deployments	Faster recovery times	Lower failure rates

Faster problem resolution	Higher employee engagement	More stable operating environments	Improved communication and collaboration

DevOps appropriately responds to this problem by evolving current systems into tighter integrations between developers and operations teams. At its core, DevOps is a cultural change that promotes collaboration and transparency. When teams agree on shared responsibility and accountability to one another, silos can be broken down and barriers traversed.

DevOps is helping to create a culture in federal IT organizations where teams collaborate using standardized processes to continuously improve and innovate. CIOs who support DevOps and have seen positive results have said an overwhelming benefit of DevOps is being able to work toward a "much faster delivery with automated server builds" and that "feature sets get into production faster."

Some organizations have reported having trouble adapting to the DevOps culture, which may have been affecting its adoption rate. The two most common issues contributing to the slow adoption of DevOps include a widespread lack of understanding what DevOps is and the difficulty of the cultural shift within existing organizations.

The four main reasons why most teams struggle to achieve the shift to DevOps is because most development teams:

- Slow down release management because they lack test automation and are not truly cross functional;
- Do not employ continuous delivery practices because they do not have automated deployments processes and tools in place;
- Do not allot enough time for continuous improvement and technical debt (the cost of additional rework caused by choosing an easy solution now instead of using a better approach that would take longer); and
- Are unable to execute upgrades and patches without taking systems offline.

Part of DevOps is also failing quickly and recovering quickly to avoid large system downtimes. A big challenge, according to one CIO, will be getting agency staff to make the mental shift that "it is okay to fail and to fail rapidly… and letting people become comfortable with [that concept]."

Despite these cultural challenges to adopting DevOps at federal agencies, there has been a sharp increase in use of a DevOps structure compared to just two years ago. Survey respondents reported two-thirds of their organizations have adopted DevOps in some part of their structure.

Cloud

This year, a majority of senior IT leaders noted several specific accomplishments and innovations in cloud adoption, showing agencies are continuing to move forward across government despite the initial resistance and requirement barriers. In 2016, while 33 percent of our CIOs responded they had implemented cloud capabilities in some capacity, and only five percent stated they felt those capabilities were "mature." This year, CIOs' confidence in this 'mature' status rose to over 19 percent while 31 percent reported "somewhat mature."

"We are increasing our cloud services. We have gone from a few dozen cloud services to 57 approved cloud services. We have also set up a cloud governance board which includes functional and customer representation. Before we had governance, we had 1,000 cloud flowers bloom and it was an expensive, risky mess."

How mature is your agency's adoption of cloud services?
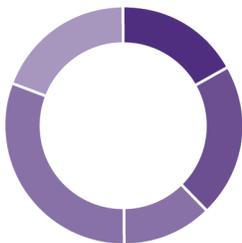
17% Not mature at all

21% Immature

12% Neutral

31% Somewhat mature

19% Very mature

How much do you agree/disagree with the following statement: *Cloud Services have provided savings and efficiencies for my agency.*

9% Strongly disagree

7% Disagree

35% Neutral

15% Agree

9% Strongly agree

25% Unknown
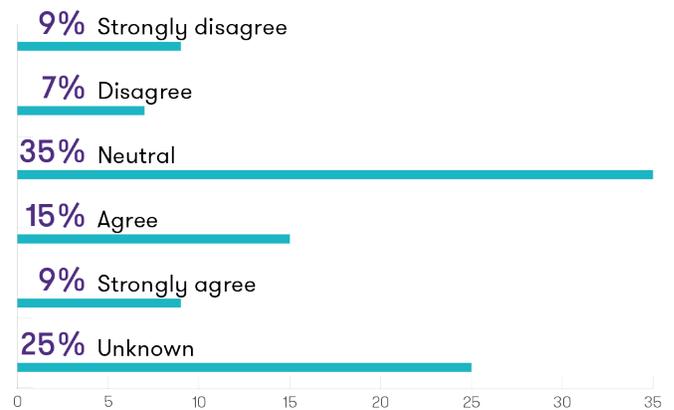
In the federal government, cloud computing is at a crossroads because of competing security requirements and the desired speed of innovation and adoption. Agencies are accepting of the innovative solutions cloud computing offers, but leadership is hesitant to migrate all of their applications, databases and complete infrastructure to the cloud because of a perceived lack of security. Existing cloud deployment models provide multiple options for productivity, connectivity, access, and security. To paraphrase one CIO, the government has made good strides in adopting cloud, but we still have a ways to go.

When asked if their agencies faced any roadblocks to the cloud, many CIOs responded with risk and data issues. One CIO asked, "who has control of the data, where does it reside and how is it accessed and protected?" Another common issue cited by multiple agencies is the OMB requirement to use Trusted Internet Connections (TIC). According to the Department of Homeland Security, this government-wide requirement was designed to "optimize and standardize the security of individual external network connections currently in use by federal agencies, including connections to the Internet." While instituting the TIC requirement in 2007 made sense, today more modern technologies, cloud architectures, and digital services

requirements have made agencies' efforts to build new services on modern platforms much more complex. One CIO said TIC is "like waiting in line at a toll booth" and creates significant latency issues.

"We are trying to operate in more places and provide our workforce with more access to the cloud, but are constrained by mandates like TIC."

FedRAMP

Since 2014, the Federal Risk and Authorization Management Program (FedRAMP) within the Government Services Administration (GSA) has aimed to accelerate the adoption of secure cloud computing across the federal government by standardizing security compliance reviews. FedRAMP's "do

once, use many times" approach includes security assessment, authorization, and continuous monitoring for cloud products and services. In the past year, the FedRAMP process has seen changes to speed up Provisional Authorizations (P-ATOs) and streamline the overall FedRAMP process to make agency coordination more efficient. Yet the continuing lack of trust when it comes to an agency relying on another agency's Authorization to Operate (ATO) or P-ATO impedes the adoption of commercial cloud solutions.

Overall, about 70 percent of surveyed CIOs believe FedRAMP changes have made agencies more effective. However, the IT community at large still has an overwhelming negative view of FedRAMP and its effectiveness. Seventy percent of surveyed professionals say the changes made to FedRAMP have not helped their agencies adopt cloud more efficiently. The assessment process includes lengthy procedures and high costs that keeps cloud service providers from receiving their FedRAMP authorization and eventually an ATO from agencies. As one CIO stated, "FedRAMP was a great idea, but GSA has lost its way by going into a more bureaucratic process. Agencies don't want to move to cloud without more security."

Thoughts on FedRAMP

In-Person

69% believe the changes HAVE helped their agency adopt cloud services

31% believe the changes HAVE NOT helped their agency adopt cloud services

Online

30% believe the changes HAVE helped their agency adopt cloud services

70% believe the changes HAVE NOT helped their agency adopt cloud services

Cloud Lessons Learned
- A complete "lift and shift" of an on-premise infrastructure to the cloud is not always the best solution.
- Moving low-impacted applications to the cloud is the best way to test an agency's adaptability to cloud computing.
- Traceability and transparency will depend on an agency's ability to track and manage data logs.
- Bringing users along the cloud journey means providing them with training and gathering periodic input on how the transition is affecting their daily operations.

Conclusion

At a time of transition, budgetary uncertainty and competition for IT talent, federal CIOs continue to push forward and attempt to do more with less resources. They must find creative ways to innovate and bring new ideas to their organizations while also meeting enduring challenges such as increasing cyber threats and maintaining mission-critical legacy systems. This year's 27th anniversary survey underscores the key role of CIOs in helping agencies meet their mission and ultimately making the federal government serve Americans more effectively.

Appendix A – List of In-Person Interviewees

Sonny Bhagowalia
Chief Information Officer
Department of Treasury

Gordon Bitko
Chief Information Officer
Federal Bureau of Investigation

David Bray
Chief Information Officer
Federal Communications
Commission

Christine Calvosa
Deputy Chief Information Officer
Federal Communications Commission

Dave DeVries
Chief Information Officer
Office of Personnel Management

Marti Eckert
Chief Information Security Officer
Social Security Administration

Steven Fine
Acting Chief Information Officer
Environmental Protection Agency

Adrian Gardner
Chief Information Officer
Federal Emergency Management
Agency

Chris Granger
Deputy Chief Information Officer
Department of Homeland Security

Margie Graves
Acting Chief Information Officer
Executive Office of the President

Vincent Groh
Chief Information Officer
Millennium Challenge
Corporation

Kris Hoffman
Principal Deputy Director, Information Technology and Chief
Information Officer
Defense Manpower Data Center

Joe Klimavicz
Chief Information Officer
Department of Justice

Steven Hernandez
Chief Information Security Officer
Health and Human Services

Kaschit Pandya
Deputy Chief Information Officer
Internal Revenue Services

Joe Paiva
Chief Information Officer
Department of Commerce

Maria Roat
Chief Information Officer
Small Business Administration

John Skudlarek
Deputy Chief Information Officer
Federal Communications Commission

Mike Tartakovsky
Chief Information Officer
Health and Human Services

Rod Turk
Chief Information Officer
Department of Commerce

Steve Warren
Chief Information Officer
Office of the Comptroller
Department of Treasury

Frontis Wiggins
Chief Information Officer
Department of State

Gary Wyckoff
Chief Information Officer
Office of Naval Research
United States Navy

Appendix B – Survey Team

Barry Adams
Parsons

Phil Agee
Attain

Naval Aggarwal
Principal
Grant Thornton

Lee Ann Anderson
Unisys

Madaline Andre
IBM

Melanie Ange
CenturyLink

Noreen Avancena
Manager, Business Development
Cisco

Cal Bassford
Senior Manager
Grant Thornton

Manish Bhatia
Technical Director
Karsun Solutions, LLC

Michael Biddick
Fusion PPT

Ken Bonner
Standard Technology Inc.

Josh Breen
Senior Manager
Grant Thornton

Michael Bruce
Director, Homeland Security
Strategic Initiatives
General Dynamic Mission Systems

Rob Buhrman
Principal
Grant Thornton

Alvaro Castillo
Unisys

Diane Ceban
SAIC

Ben Clark
Northrop Grumman

Thomas Coleman
IBM

Mary Ellen Condon
Director
Condon Associates LLC

Lou Crenshaw
Crenshaw Consulting Associates

Asia Dawson
Lead Associate
Heitech Services

George DelPrete
Principal
Grant Thornton

Giovannina Dipietro
HHS Client Relations Executive
Optum Federal Solutions

Martha Dorris
Dorris Consulting International

Charmaine Edwards
Microsoft

Mary Margaret Evans
LMI

Amy Fadida
President and Chief Executive
Officer
A.M. Fadida Consulting

Joni Fernbaugh

Heather Frazier
General Dynamics Information
Technology

James Gaul
Accenture Federal Services

Richard Giebel
AT&T Government Solutions

Brenda Girod
DOE Lead
ICF International

Derry Goberdhansingh
e3 Federal Solutions

Gayle Grasso
Client Executive
IBM

Appendix B – Survey Team

Robert Haas
Director, Strategy
Hewlett-Packard Enterprise

Elaine Haemisegger
ICF International

Dean Halstead
SAIC

John Hamilton
AT&T

Kimberly Hancher
Deep Water Point, LLC

Kristin Hug
DRT Strategies

Adam Hughes
Director
Grant Thornton

Tricia Iveson
CEO
10novate

Michelle Jobse
PSC

Sheree Jones
IBM

Steven Katz
Senior Manager
Grant Thornton

Kitty Klaus
Hewlett-Packard Enterprise

Kathy Lentz
Founder and President
Federal Insights, LLC

Clifford Lowrie
Director
Deloitte

Angela Martin
Unisys

David Martin
Account Executive
Teradata
Government Systems LLC

Felix Martinez
Deloitte

Joshua McGee
Sr. Associate
Grant Thornton

Dave McGinn
Client Sales Executive
Hewlett-Packard Enterprise

Marianne Meins
Parsons

Michelle Montoya
Manager
Grant Thornton

Rebecca Moss
Lockheed Martin

Deirdre Murray
Director, Business
Development
CenturyLink

David Newberry
Business Development
Leidos

Ken Newcomer
ICF International

Tim O'Brien
Enlightened Inc.

Todd Pantezzi
Vice President
ICF International

Dawn Platt-Pembroke
Principal
Grant Thornton

Larry Reagan
Maximus

Bradley Saull
PSC

Glen Sears
Lockheed Martin

Matt Shankle
Sr. Associate
Grant Thornton

Dave Simprini
Principal
Grant Thornton

Susan Smoter
Business Development Executive
Hewlett-Packard Enterprise

Sean Spann
CTO
Buchanan & Edwards

Lori Stallard
Vice President, Business
Development
Leidos

Mary Swann
Business Development
Manager, Foreign Affairs
IBM

Simon Szykman
Attain

David Tamayo
Chief Information Officer
DCS Corporation

Wei Tang
Director
Grant Thornton

Kathy Taylor
DRT Strategies

Richard Thielen
CenturyLink

Kate Thomas
CGI Federal

Steve Vetter
Cisco

Mike Vogel
Kforce Government
Solutions

Janet Webb
SAIC

Bob Wells
Cubic

Antoinette Williams
Consultant
Federal Insights, LLC

Kathryn Woodward
General Dynamics

Acknowledgements

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

PSC **PROFESSIONAL SERVICES COUNCIL**

Grant Thornton