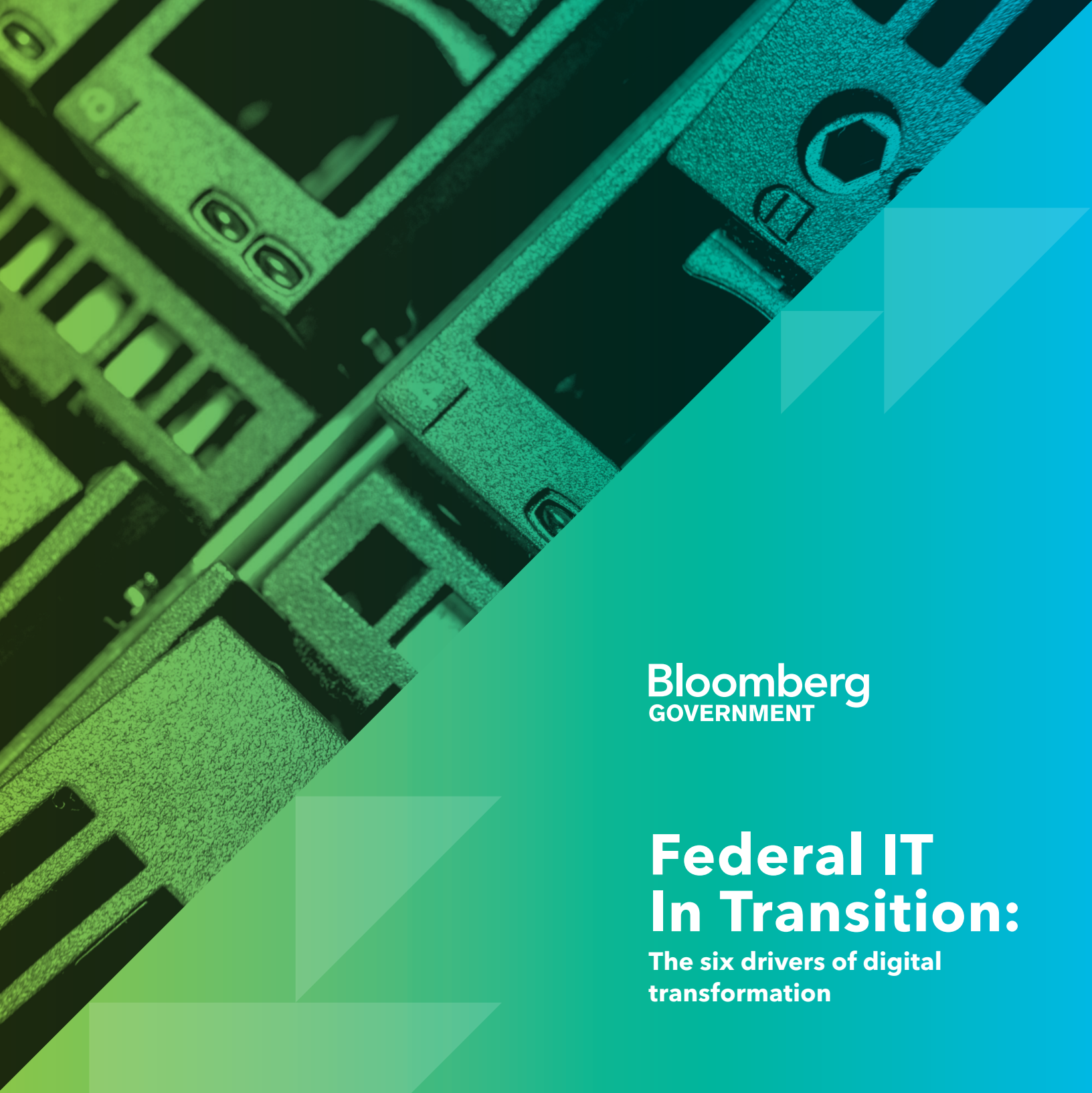


Bloomberg
GOVERNMENT

Federal IT In Transition:

The six drivers of digital transformation

Sponsor Content

CISCO

Reimaging Government:

Implementing the six drivers of digital transformation

Major technology trends such as mobility, big data, analytics, Internet of Things and cloud solutions offer a new paradigm for federal agencies to reimagine government. Technology driven transformation offers government agencies an opportunity to digitally disrupt their organizations to drive deep reform of service delivery, improve business operations and adopt new and agile technologies. Government's IT leaders confront a long list of challenges on their path to digital transformation, including the priorities of the new presidential administration, aging and complex infrastructure, budget uncertainty and constantly changing security regulations and threats.

Many agencies have made significant progress in their digital journey, though an overwhelming majority are still in the early or developing stages of their full-fledged digital transformation.

A change of presidential administration and Congress always brings uncertainty to agencies, as leaders wait to see which programs from the past will continue, which will be canceled, what new ones will be created and how priorities will shift.

Nevertheless, IT leaders must continue to deliver on their mission, address critical security vulnerabilities and drive the adoption of new digital technology solutions that will accelerate the transformation of their complex organizations to deliver more agile, secure, personalized and cost-effective service experiences to customers.

This guide will help you explore the six key building blocks to digital transformation—crucial drivers that government leaders must address as part of an overall agency strategy required to advance your mission, realize the wide-ranging benefits that come with digital transformation and ultimately deliver on the promise of a more citizen- and customer-centric government. These six foundational drivers of digital transformation provide federal agency leaders with a firm foundation for the next four years, while enabling them to build the capabilities needed to meet future expectations.

Table of Contents

Driver I:

Security & safety

If you're a federal IT leader, you already know the cyber threat is real and pervasive. As every agency's cyberattack surface area increases in size and complexity, the question is how to manage it all. The answer? A meaningful cybersecurity architecture.

QUICK TAKE:

- **A robust cybersecurity architecture is required for every agency—and federal IT leaders need to lead the charge by eliminating silos and getting everyone at the table to contribute to the agency's cyber strategy.**
- **As digital endpoints expand, so do the risks. Federal IT leaders need to think beyond cyber and incorporate physical security into their security architecture.**
- **Beware of the insider threat. Whether they act out of malice or simple ignorance, your own employees and contractors can do tremendous damage.**

To be a federal IT leader today is to oversee amazing possibilities—and terrifying security risks. Heightened connectivity has improved access to government while dramatically increasing the complexity of the cybersecurity risks agencies face. Whether it's nation states, independent hackers or employees who inadvertently imperil agency security, federal IT leaders face more risks than ever simply due to the perpetual expansion and modernization of agency infrastructure.

So, what can you do to protect your agency?

The first thing to remember is that you, as an individual, can't do it alone. The cyber threat is so complex and so diverse that it requires a convergence of roles and responsibilities. The entire federal technology C-Suite needs to systemically join forces with all leaders responsible for security in the organization. Now is no time to be territorial.

The playing field for attackers grows ever larger thanks to new technologies such as cloud computing and the Internet of Things. In addition, many agencies trust their security to multiple vendors, creating an environment which is complex and tricky to manage, and not necessarily more secure.

Another challenge of IoT is that its endpoints are geographically diverse—think remote weather sensors, or a monitoring system in a military vehicle—and leaders responsible for physical security are more important to your cyber strategy than ever before.

In short, your cyber-attack surface area is rapidly expanding. To take back control, federal IT leaders need to invest in a meaningful security architecture, rather than a piecemeal approach. A security architecture is the only way to create a comprehensive strategy and automate its execution.

Strategic Takeaways

1. **A security architecture is a crucial methodology.** It is how you optimize your existing security tools, account for your risks and the leaders who manage them, and design processes that identify potential weaknesses before, during and after a breach. The right architecture, combined with adherence to the appropriate security standards, will drive your ability to achieve pervasive security. You won't stop every threat—but you'll have the peace of mind knowing your agency is prepared to respond when the inevitable happens.

2. **Focus on converging roles and responsibilities across the enterprise—including the integration of cyber and physical security.** In the effort to digitally transform your agency, "security" is a holistic and streamlined concept. The walls between physical and cybersecurity have fallen—which means all security leaders need to come together. In a world where cyber threats target critical infrastructure like power grids, there's no room for silos. Your cybersecurity architecture needs to facilitate this cultural transformation and get the right leaders in the right room at the right time, working together to create a strategy that integrates the physical and the digital.

3. **Don't ignore the insider threat.** High profile leaks of classified government information are on the rise—and it's these intentional and malicious actions that most come to mind when we think of "insider threats." But as digital connectedness in agencies is increasing, unintended and accidental actions of employees that expose the agency to security risks are also rising in lockstep. A lost laptop, a phishing attack, an insecure password—employees can potentially do more to thwart your security strategy than any intentional cyber-attack. Your security architecture needs to incorporate insider threats, establishing robust governance policies and effective monitoring systems to determine what's normal, what's negligent and what's potentially malicious in your agency's environment.

4. **Adopt a value chain-centric approach to security:** Information technology and operations technology are converging in this digitized world. It is not enough for government agencies to focus only on protecting their internal business models, mission offerings and infrastructure. Federal IT leaders must look at their security value chain holistically to ensure that the right security is in the right place at the right time, from end to end, for hardware, software and services. This value chain-centric approach helps ensure that security considerations are built into every stage of the solutions lifecycle.

21 Million

The number of former and current federal employees whose private information was exposed to foreign hackers in the 2015 OPM cyber breach.

44%

The percent of endpoints that federal IT leaders say are unknown or undetected, according to a MeriTalk survey.

Driver II:

Applications & infrastructure modernization

Application and infrastructure modernization is critical to achieving agency mission and operational objectives. But it's a mistake to see it as nothing but an effort to adopt the latest and greatest technologies. Modernization is a strategic effort—it requires a digital strategy and leaders with an enterprise approach. In the past, modernization might have meant replacing a dot matrix printer with a laser printer. Today, digital technologies provide agencies with the opportunity to ask: "Do we even need the printer?"

QUICK TAKE:

- **Agencies continue to spend about 75 percent of their IT budgets on operations and maintenance, rather than development and modernization. Every agency has to balance maintaining the old with adopting the new.**
- **Many agencies are juggling dual modernization strategies: bringing in new technologies to improve services, while simultaneously maintaining some legacy systems.**
- **Application rationalization gives agency IT leaders an opportunity to review their entire portfolio and determine what they really need to fulfill their missions. Eliminating unneeded applications is as much a part of modernization as implementing new systems.**

Infrastructure modernization in the federal government is akin to changing tires on a moving car. Approximately 75 percent of agency information technology budgets go toward operating and maintaining legacy systems rather than modernizing them—which means, if you're a federal IT leader, you've likely come to accept the reality that every agency has to integrate modern systems side by side with legacy systems. The longer you hang on to legacy systems, the longer they have to contend with the security and operational drag of unsupported hardware and software, lack of security updates and the inability to deliver the right services to citizens and stakeholders.

So what can a federal IT leader do?

First, recognize that much of what ails you is out of your hands. Slow-moving procurement processes, constantly changing security regulations and a lack of skills in the workforce—all are key components (and challenges) of application and infrastructure modernization that plague leaders across every federal agency.

You have to take an enterprise view of the challenge. Where possible, opt for solutions that fit into the larger enterprise, rather than "purpose-built" solutions that address only one problem. Prefer open-source solutions over proprietary systems as much as possible.

Finally, take time to understand the underlying problems you are trying to solve and the details that pertain to a particular situation—always with an eye toward the overall enterprise strategy—before adopting new technologies. Not every cloud infrastructure is ideal for mission-critical agency applications, for example. Modernization is about supporting workflows and making service delivery more efficient, not just bringing in new tools.

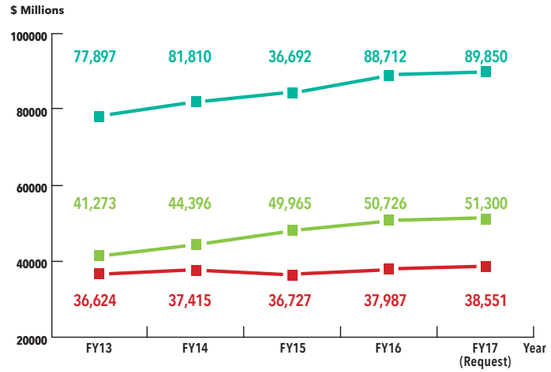
Strategic Takeaways

1. **Ensure your digital strategy is comprehensive.** Want to learn how digital-ready your agency really is? Building your digital strategy will help you assess priorities for modernizing your infrastructure. An enterprise-level digital strategy encompasses a range of initiatives such as developing new services, re-engineering governance and the core digitization of public services. The most important aspect of the strategy is not the technology; it's creatively reworking business processes to make the most of the new technology.

2. **Embrace agile and open-source development to boost enterprise-level interoperability.** With a comprehensive digital strategy built, agile development techniques can help you execute with an enterprise-view and break down information silos—avoiding those costly "purpose built" solutions when an open source approach might benefit the entire agency. Furthermore, agile puts customer experience front and center, ensuring your modernization efforts actually deliver for your stakeholders. Veterans Affairs has used an enterprise approach to transform how it includes veterans in its modernization efforts, GSA's 18F has led the way on helping its agency stakeholders adopt agile methodologies, and U.S. Citizen and Immigration Services has used agile and design thinking methods to transform the citizen experience with its e-verify systems.

3. **Cloud-optimize your infrastructure.** Agencies are being driven into the era of cloud computing and modern infrastructure by several conspiring policy forces. OMB's Data Center Optimization Initiative (DCOI) is accelerating movement toward cloud by mandating that agencies reduce physical data center costs by 25 percent in FY2017. A hybrid cloud approach is a good first step for many agencies. It enables an agency to balance isolation, cost and scaling requirements. At the end of the day, cloud is the future and on the rise—but leaders need to strike the right balance between on-premise and off-premise cloud solutions.

Federal IT Spending (In Millions)



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

75%

The amount of agency IT budgets that go toward maintaining legacy systems, instead of development and modernization efforts.

Driver III:

Big data and analytics

The government of the future uses big data to unlock new ways of serving its stakeholders—but getting there remains a challenge. Here's what you need to know as you consider incorporating big data analytics into your digital transformation strategy.

QUICK TAKE:

- **Before you pursue analytics and big data solutions, make sure you understand the distinction between business intelligence and big data analytics—as well as the problem you're trying to solve.**
- **With big data analytics, mileage may vary. Your infrastructure may limit the velocity with which your agency can gather and analyze data. Storage in particular can complicate matters.**
- **Security in all things. As we've established, new endpoints mean new risks. And big data analytics can introduce new security risks to your agency if not managed from the beginning.**

Among IT executives, "analytics" and "big data" are pretty slippery terms—they can be shorthand for practices that don't fit the actual definition of analytics (i.e. having an Excel wizard on your team doesn't mean you have "analytics" in the way we'll be discussing it). To talk about what big data analytics is, let's first talk about what it is not.

Many agencies are still in the early stages of determining how analytics solutions can provide actionable insights from their ever-growing stored data sets and still effectively govern and secure huge volumes of information. Other agencies are already well equipped to collect data, but are still figuring out how to make the data actionable by improving the quality and scope of what gets analyzed. Agencies like Centers for Medicare and Medicaid Services, the U.S. Census Bureau and the IRS are seeing the benefits of big data analytics in driving enhanced operational outcomes and delivering on their mission.

The journey to leveraging big data analytics within your agency starts with understanding the problem you're trying to solve. Specific analytics problems have specific analytics characteristics and needs. For example, cybersecurity analytics monitor network activities and behaviors to identify known and suspicious patterns of access indicative of a breach. This requires your agency to gather data from numerous data streams with a wide range of structure, format and content (e.g. Domain Name Servers [DNS], Dynamic Host Configuration Protocol [DHCP], NetFlow, web logs, alerts, configuration data, audits, emails, and social networking data flows). On the other hand, analytics to detect fraud, waste and abuse requires the absorption and analysis of massive amounts of transaction history data.

The point is, analytics are the precursor to actionable insights—and therefore an essential ingredient for any digital transformation initiative. Analytics allow you to make the invisible visible, meaning it allows you to discover hidden connections and really start optimizing processes or reinventing them altogether. In the end, the ability to leverage data more effectively allows you, the federal IT leader, to deliver better customer experiences—and that is the quintessential goal of digital transformation.

Strategic Takeaways

1. **Understand the problem you're trying to solve first.** Common federal use cases for big data analytics include cybersecurity, personalization of customer experience, operational insight and the analysis of fraud, waste and abuse. However, big data analytics is not a one-size-fits-all solution; each problem has specific analytics characteristics and needs. It's essential to capture the right data points, analyze them with the right tools and interpret them via people with the right skills.

2. **Ensure your IT infrastructure can support big data analytics.** Consider features such as in-memory computing for a solid analytics foundation. Open source platforms tend to be preferred as they also provide scalable solutions. However, remember the guidance above to factor in the specific need or problem to your decision-making. Storage can present IT leaders with significant challenges, especially when unstructured data is involved—and that's one key potential use for cloud solutions.

3. **Embed security needs into the overall analytics architecture.** Big Data expands existing information security responsibilities and introduces new risks. Ensure data is secured from every angle—from firewalls that guard against intrusion, to user-authentication to fight the insider threat. Big data analytics implementations also often include open source code, with the potential for unrecognized security risks, back doors and default credentials that must be changed to be secure. For security and privacy alike, your security architecture should address policies and controls.

The White House Office of American Innovation

On March 26, President Trump announced a new White House office focused on applying private sector and business lessons to the federal government. The office is largely focused on technology and data, and is collaborating with Apple, Microsoft and Salesforce executives. Keep an eye on this new office over the next several months and its implications for Big Data Analytics.

Big Data:

Traditionally described as high-volume, high-velocity and high-variety information.

Big Data Analytics:

Usually involves large quantities of structured and unstructured data and uses sophisticated algorithms to drive decision-making.

Predictive Analytics:

Algorithms that help analysts predict behavior or events based on data.

Cloud Analytics:

Analytics tools and techniques specifically designed to extract information from massive data sets using cloud-based processing power.

Business Intelligence:

Involves gathering, storing and providing access to data through applications.

Driver IV:

Customer experience

Customer experience is all about effective, efficient and seamless delivery of services. Agencies are becoming more customer-focused by delivering human-centric services at a lower cost. With the growing move to digital channels, innovative self-service tools and new delivery platforms, agencies are removing obstacles and responding to customers' demands for different ways to engage with government.

QUICK TAKE:

- **Customer experience is transforming how agencies design services—and how citizens and agency stakeholders alike experience working with the federal government.**
- **Agency leaders need to invest time into understanding their customers' end-to-end journey. Only after talking to actual customers and empathizing with their pain points should time and resources be invested into designing solutions that solve those issues.**
- **IT leaders should look at where in their service blueprint customers experience breakdowns and transform those into opportunities to build stronger relationships through better service delivery.**

All of the drivers of digital transformation matter—but perhaps none more than customer experience. Agencies are taking the best of modern design and software development techniques to become more customer-centric. Coupled with mobile apps, secure networks and the power of the cloud, this boom in citizen-centered approaches has resulted in a revolution in how federal IT leaders approach service design and delivery.

Across the federal landscape, numerous examples represent the tip of the iceberg of what's possible via a customer-centric government. Examples of redesigned government services include an overhauled Vets.gov, which helps veterans find and use the services they've earned; a streamlined U.S. Citizenship & Immigration Services (USCIS) experience, which helps process immigration requests faster; and the launch of College Scorecard through the Department of Education, which helps high school students better understand their higher education options.

Through this commitment to an improved customer experience, digital transformation becomes real—whether the "customers" in question are government employees, members of the public, other agencies or state and local government organizations.

Strategic Takeaways

1. **Understand your customer's end-to-end journey.** The science of customer research has come a long way. IT leaders have access to a range of design techniques that they can use to ensure they are ready to build software and services that people actually want. This means you've got to do research—and talk to actual end-users. Customer journey maps are an effective tool to understand customer behavior. (Check out Usability.gov for more techniques) Only after you understand the customer's experience should you get to work building solutions to address their needs. Taking the time to identify and prioritize needs allows leaders to focus time and resources on truly needed changes.

2. **Transform your contact center into a relationship hub.** For many customers, their first point of contact with government is through contact centers. Traditionally, these have been cumbersome, frustrating experiences—processing centers for general customer questions with no guarantee the person on the phone can actually help. Many agencies are turning these contact centers into "relationship hubs," places where streamlined customer service approaches can make for a much better experience. To achieve this, agencies are embracing a customer's multi-channel reality—enabling them to contact an agency through any combination of voice, email, web chat and social media.

3. **Implement self-service tools where you can.** Self-service tools and virtual agents provide a more convenient experience for customers. According to Forrester, self-service tools can drastically lower costs—from $12 per service interaction to 25 cents. Virtual agents on mobile devices can deliver customers relevant, personalized service advice that, when necessary, can advance to a live agent who is already aware of this interaction history. In the end, it's about respecting a customer's time and removing obstacles between them and the information they need.

$26 Billion

The amount the federal government is expected to invest in customer engagement technologies in 2017.

The 13 essentials of public sector customer experience from the Digital Services Playbook:

1. Understand What People Need
2. Address the Whole Experience
3. Make it Simple and Intuitive
4. Build Services Using Agile
5. Structure Budgets to Support Delivery
6. Assign One Leader
7. Bring in Experienced Teams
8. Choose a Modern Technology Stack
9. Deploy a Flexible Hosting Environment
10. Automate Testing and Deployments
11. Manage Security and Privacy Reliably
12. Use Data to Drive Decisions
13. Default to Open Standards

Driver V:

Sustainability & real property

In the quest for a more cost-effective government, several initiatives have made significant strides in reducing the government's energy footprint. But, nevertheless, energy inefficiency remains a significant economic drain—and digital transformation holds the key to innovative ways of reducing costs and driving the efficient use of resources.

QUICK TAKE:

- **Implementing sustainable IT business practices is a growing focus for federal agencies and critical to a renewed focus on agency-wide cost savings.**
- **Since 2010, the government has had major success in reducing its power consumption and emissions thanks to a cadre of data center consolidation initiatives.**
- **The average data center consumes the same amount of energy as a medium-sized town in the U.S.**

The federal government owns more than 900,000 buildings and structures with a combined area of over 3 billion square feet. In 2012, the government spent $33 billion in total operating costs of real property and spends $4.2 billion renting office space each year. Beyond property, the federal government is also one of the largest energy consumers in the world. In FY13, U.S. government vehicle and equipment energy usage accounted for 62 percent of all the federal energy consumed—with the remainder used by federal facilities. Going a step further, the U.S. government also owns data centers—which, by design, consume vast amounts of energy. In FY14, the government spent approximately $5.4 billion operating physical data centers.

The moral of the story? The federal government is the country's largest property owner—and sustainability is critical, not just for its impact on the environment, but for the effect it has on cost reduction and enabling the workforce of the future.

In an environment characterized by high energy costs, budget uncertainties, a shortage of qualified staff and constant technology changes, the demand to improve data center performance is a continuing challenge. Whether an agency wants to take advantage of virtualization or move to the cloud, it must have a holistic view of its data center functions and address all key aspects of data center transformation including infrastructure, virtualization and automation.

Taking a lifecycle architecture-based approach provides a framework for agency IT to understand the complex moving parts of a data center and to plan, build and manage its data center transformation on the journey to cloud. This approach helps an agency evaluate its current data center environment and assess costs related to infrastructure migration and management. It also prepares the data center for end-to-end virtualization by identifying gaps in the server, storage and network infrastructure. The resulting consolidated and optimized solution will offer the agency IT organization dynamic efficiencies that can accelerate savings and make its data center easier to manage and scale.

Strategic Takeaways

1. **Continue to enable and support a remote workforce.** Beyond offering employees flexibility, a remote workforce can mean significant cost savings. Remote workers require less physical office space, and when energy usage and sustainability are factored in, the cost reduction is even more significant—estimated at an average saving of $10,000 per employee per year. There is more to it than just approving work-from-home arrangements, though. Digital transformation means having the right tools and infrastructure for the job. Agencies should implement a stringent process to determine which employees are eligible to telework successfully. To ensure they're successful, agencies need versatile and secure collaboration and communication tools to connect managers and teams.

2. **Leverage workplace modernization efforts.** Many buildings in the Federal Real Property Portfolio are more than 40 years old. They have aging mechanical equipment that performs inefficiently and with a high failure risk. In modernizing buildings, many agencies are exploring net-zero design, advanced building technologies, smaller environmental footprint options and innovative workplace solutions. IP and Power over Ethernet (PoE) are being used to converge building networks and services (e.g. lighting, climate control, security, etc.). It's ultimately not just about creating connected buildings—but about implementing smart buildings.

3. **Continue the push for data center optimization and consolidation.** Data centers are expensive. Federal IT leaders need to take a holistic view of their data center functions to prioritize their data center transformation initiatives including infrastructure, virtualization and automation. Lifecycle architecture-based approaches can help an agency evaluate its current data center environment, concerns and costs related to infrastructure migration and management. In lieu of data centers, federal IT leaders should continue to push for ultra-agile infrastructures. This includes fully exploring the possibilities of technologies like data center virtualization, software-defined networks (SDN), network function virtualization (NFV), cloud, automation and management tools.

900,000

The number of buildings the federal government owns and operates, totaling 3 billion square feet as of FY12 (Source)

$4.2 Billion

The amount the federal government spends on renting office space each year as of FY12 (Source)

$10,000

The amount per employee per year the federal government saves in energy costs for each remote worker (Source)

Driver VI:

Next-generation workforce

Federal managers are entering a new era of austerity, with budget cuts and hiring freezes again becoming part of the realities of federal service. Now leaders need to button up their strategic plans, prioritize and prepare—again—to do more with less.

QUICK TAKE:

- **With President Trump's determination to reduce the federal workforce, managers should expect their ability to hire new talent to be severely curtailed as the administration takes shape. This makes it doubly important for federal managers to keep the talent they already have.**
- **Even in an austere environment, good management remains essential to employee satisfaction. It's on federal IT leaders to match their employees to the right task, find opportunities to get their current staff trained and to lend an empathetic ear in times of stress.**

Federal employee engagement—a measure of how satisfied and involved federal workers feel—was trending upward when President Donald Trump took office, after trending downward for most of former President Barack Obama's second term.

Though the public sector still lags the private sector in satisfaction, one could assume that the new administration, with its private sector bonafides, would be a good fit for a federal workforce on the rise. But the opposite will likely be true—with promises to "drain the swamp," an executive order freezing all new hires by the federal government (except in the military) and a presidential budget request so austere it is expected to dramatically shrink the federal workforce. Federal managers are likely to see a worsening of engagement and morale for the foreseeable future.

It doesn't have to be that way, though. Federal IT leaders were already working on digital transformation, and the new president's reluctance to expand the federal workforce only puts that much more urgency on digital transformation's potential for efficiency and automation. The era of "do more with less" is back in force. To make the most of it, managers need to align their resources to value-added tasks, embrace automation where possible and more than ever, work with what they have—making sure their existing employees have, or are retrofitted with, the right skills.

Strategic Takeaways

1. **Get serious about your strategic plan.** Bring together all your stakeholders to plan and prioritize what and what not to spend your limited budget resources on. Reinvest in analytics and performance management systems that help you track what you're doing and how you're spending. The demand on your resources only grows with time, but your team can't do it all. In other words, "do more with less" simply means prioritize.

2. **Ensure employees have the right skills for the right jobs.** A good strategic plan goes hand in hand with smart workforce planning. Seek your existing workforce planning frameworks within your agency to assess the skills on your existing teams to identify gaps. In these gaps, consider realigning resources, bringing in new training programs or looking cross-departmentally for shared resources you can leverage to address gaps that affect your essential functions.

3. **Nurture and retain your top talent.** At the end of the day, remember you are a leader within your organization. People look to you for direction and support. It's easy to grow cynical in the face of budget cuts, but your attitude and model have more to do with employee morale and engagement than you think. Take time to check in with your employees, listen to their concerns and fight for resources to give them training and opportunities that help them grow. Your hands may be tied on many issues—so good, empathetic management is more important than ever.

210,000

The average number of jobs turned over in the federal workforce over the last five years. Of those who left, 75,000 quit, 65,000 retired, 55,000 left because of expired appointments and 10,000 were fired. (Source)

1/5

The fraction of the federal workforce expected to be affected by President Trump's memorandum in January 2017 freezing federal hiring, approximately 800,000 employees. (Source)

Finishing what you started:

Continuing your digital transformation journey

Digital transformation won't happen overnight, but making advances across these six components ensures federal IT leaders are leading their agencies toward a better government.

No organizational transformation is easy or smooth. When you add in the unique demands of running a federal agency, it can seem like the digital future is far off indeed. But federal CIOs have already demonstrated their innovation, drive and commitment to their missions in the advances they've previously made.

The six drivers of digital transformation are designed to help agency leaders move the chains downfield in creating a government that serves citizens and customers better. Over the last several years, federal IT leaders have led the charge toward this digital transformation. To maintain momentum, these six interconnected drivers are essential to completing what you've already started.

As the new administration gets underway, federal IT leaders should continue to build on their successes and work with the new administration to find better, faster and more creative ways of leveraging technology to change the way agencies do business and respond to citizen and customer needs.