

---

# Why Government Needs a Holistic Approach to **IT Modernization**



---

# Introduction

IT modernization is a mammoth topic in government, and as such, no department or agency can tackle it alone. Agencies are battling against their legacy systems, constantly updating at the price of innovating, and employees across government are frustrated.

Government leadership is worried about the costs of modernization versus the wasted costs of maintenance. IT departments fret about reacting to potential systems crashes or data breaches. Procurement officers struggle to find the right fit and have to cope with the consequences of bad contracts and systems.

And finally, end users just want a system that lets them get their work done.

In June 2019, GovLoop, Verizon and Amazon Web Services (AWS) hosted a roundtable event that allowed public sector employees and leaders to discuss their top challenges and potential solutions for IT modernization. Bill Zielinski, Acting Assistant Commissioner in the Office of Information Technology Category for the General Services Administration (GSA), and Michael McFarland, Director of Acquisition Business Systems for the Health and Human Services Department (HHS), spoke to attendees and answered questions at the event.

They were joined by Jamie Baker, Senior Manager of Federal Civilian for AWS, and Steve Lefrancois, Public Sector Chief Technology Officer for Verizon.

The following sections will recap five main takeaways from the event and provide color to what attendees and speakers had to say, offering current examples and policies related to IT modernization.

---

---

# Table of Contents

- 4 Putting Progress Ahead of Process  
Tips for Innovators
- 6 Focusing on Users While Incorporating New Technologies  
Tips for Leadership
- 8 Clearing the Way for IT Modernization With Data  
Tips for IT Employees
- 10 Bringing Emerging Technologies to Life to Empower the Workforce  
Tips for End Users
- 12 Setting Aside Security Fears to Focus on Upgrading Systems  
Tips for Security
- 14 How AWS and Verizon Can Help
- 15 Conclusion



# Putting Progress Ahead of Process

The first step to IT modernization might not be an addition to tech portfolios or a big-money program. Instead, agency personnel – and just as importantly, agency leadership – must recognize that IT modernization isn't a choice; it's necessary to deliver services going forward.

Employees are being asked to do more and more with existing legacy systems. Disruption is needed, and end users of IT systems know it better than anybody.

"It's the same problems everyone else has – old systems, old processes," McFarland said of the challenges that crop up at HHS.

In government, however, inertia often wins the day. For every subset of the workforce that's ready for new systems, an opposing force resists change. At the IT modernization roundtable, several employees across different levels of government suggested one of those primary departments that proves to be a roadblock is IT, where employees are often familiar with a particular set of solutions and hesitant to pick up anything that would fundamentally change the shape of their work.

"The words that kill a lot of things are: 'This doesn't fit our architecture,'" McFarland said.

One attendee, an engineer from a mid-sized state agency, said it was too difficult to get things done by going through IT. "They never have time. They don't listen to what you say," she said. Expressing the inefficiency, she used the analogy that IT wanted her to travel by donkey instead of by airplane.

Many attendees at GovLoop's IT modernization roundtable expressed the same frustration with their IT departments. They suggested IT departments halted new projects and slowed progress out of technical, procedural concerns instead of considering big-picture gains that new technologies, systems and processes could bring into the fold.

Employees who went to the event considered potential fixes. An employee of a small federal agency proposed that the only way to get through to IT was to work around the department entirely.

"It's almost to where you have to circumvent the existing IT teams, particularly the ones who resist change, because they hang on to the servers," that employee said.

## Tips for Innovators



- Begin with a small pilot program.
- Stoke support from a single member in every team, and present the business case to leadership, without focusing on technicalities.
- Start with a small but meaningful system and try to expand the pilot over time.

This approach, known in some corners as “shadow IT,” is one that many in the room nodded their heads in agreement with and found to be effective.

To actually bypass IT requires a concerted effort and a lot of support from the top and around the agency. Leadership and procurement would have to OK the purchase of a new system and plan to phase out an old one without going through IT checks or reviews. Once the system was in place, IT would have to “deal with it.”

Even if effective, that approach might not be feasible in most government environments, as it requires widespread support and constructs a very adversarial base for future relationships with IT. Another approach, however, has been effective in HHS and GSA.

“Just start with a small little pilot,” McFarland said. “Who has issue with that? And then you start showing value, and as people start to see value...it builds momentum.”

These pilots, which often can take just \$50,000 of seed money, are important mechanisms for agencies to test value and foster support for solutions before going all in on a divisive system. Pilots can foster support from all corners, even IT.

At HHS, Jose Arrieta joined the staff from GSA with a pilot idea to modernize the acquisition system by tracking inputs and, in the future, automating contracts using blockchain technology. When GovLoop spoke with him in January 2019, he praised leadership for providing the support.

The pilot became an official program, earmarked for 896% return on investment, and Arrieta became the chief information officer (CIO) for HHS. The program could revolutionize contracts and is on course to save HHS tens of millions of dollars.



# Focusing on Users While Incorporating New Technologies

Although in many situations the case for IT modernization is clear, employees can still have difficulties adjusting to new systems. Even if they're in favor of larger modernization efforts, when change fails to be communicated properly and affects them, employees' questions about the transition can quickly fester into concerns.

As mentioned in the previous section, blockchain, a digital ledger technology that immutably tracks and stores inputs into a record, is disrupting HHS and GSA by transforming the procurement process.

But before HHS explained why it selected blockchain, many contracting employees didn't know what to make of the technology and its adoption. In fact, blockchain, a major change to the systems they were used to working with, was foreign and threatening.

*Will I know how to use the new systems? How much meaningful work will be left? Is my job being replaced by robots?*

"They have that trepidation of, 'OK, what's going to happen to me?'" Zielinski said.

That's why when implementing systems, communication and stakeholder engagement is required to undergo a successful transformation.

McFarland has found that some of the best ideas for improving systems that are being upgraded have come from employees who were skeptical of the change initially. After learning more at town halls and information sessions that HHS holds, they can contribute to and even embrace what's coming. McFarland said that the series of demonstrations HHS held was so popular that they received requests from all across departments to see videos of the new system.

Contracting personnel were not "married" to acquisition systems, McFarland said, but they needed the explanation to be comfortable. Then, 1102s, or government contracting professionals, quickly became excited to adopt the new blockchain technology and all of the perks – such as artificial intelligence to analyze and inform contracts, freeing up employees to do higher-value work.

IT modernization is vital for government success, but questions about new systems are understandable and usually legitimate. Sometimes, the human capital piece gets lost in these transitions.





People who advocate for IT modernization can easily turn into cynics when the change is not clearly communicated. Getting people who are using these systems on board with the plan is the only way to tackle all potential concerns.

Therefore, agencies need a strong stance on modernization while incorporating an open-door policy for those affected.

“We’re going to do this. We are,” Zielinski said, emphasizing that strong leadership needs to be at the forefront of IT modernization efforts.

What strong leadership means is engaging employees from the start of the process to the end. GSA has built out peer engagement groups, inviting members from different departments to give feedback on systems and processes or weigh in on potential upgrades. While change is needed in the government, the process can always be improved by having a diversity of voices from different branches of business.

User groups, demonstrations and town halls are ways government can do just that. Therefore, GSA has expanded its programs to engage representatives from their external customers – people from different departments in other agencies who could soon use the systems.

Leadership needs to be resolute that change is coming, and focus on offering employees actionable steps, open communication and accessible training when it comes to new technologies. Doing so will elicit the best processes, as users on the ground will know what should go in place with these systems better than leadership could alone.

### Tips for Leadership



- Clear and decisive direction from the top is needed to push any substantive change through large organizations, but authoritative despotism is sure to kill off new projects.
- Ensure that you’re putting systems in place – town halls, messaging boards, information sessions and more – to allow employees to help decide what change is needed and how it should be implemented.

# Clearing the Way for IT Modernization With Data

IT modernization is like working on a house. Sometimes, changes only need to be incremental, like small plumbing repairs, or cosmetic, like fresh paint jobs. Other times, you need a whole overhaul of what you're working with, like tearing down and starting over altogether.

In this situation, governments need the works, and while IT modernization comes in many different shapes and sizes, it all starts with a strong foundation. And for government, that foundation is data.

"Data is the lifeblood of what many of our agencies are here to do," Baker, who joined AWS from the federal government, said at the roundtable.

Data is a constant for every single agency, but its presence alone doesn't do all that much. The data that matters most is actionable data, something that the federal government has struggled to keep up with. It's a chicken-and-egg problem, McFarland said; the systems need to be in place to show the business value of data, but the only way systems are effective is if they're powered by clean data.

While hoarding massive amounts of data, many agencies often waste what they have, as old systems can't utilize new data that's constantly being collected with digital forms or Internet of Things (IoT) sensors. Furthermore, federal data, by and large, isn't usable. The data is often filed and coded independent of standards – both across departments and sometimes by different people with the same job – and it's stored in unsociable formats.

"We're living in PDF hell," Zielinski said, referring to a format where data cannot be processed or easily extracted, as opposed to in a spreadsheet.

IT modernization hinges on data and all of the systems that surround it. IoT devices send frequent packages of data back to agencies, and 5G wireless networks are being built to support the rapid flow of data between systems. The newest IT systems, such as machine learning and robotic process automation (RPA), depend on the availability of actionable data immediately, and with modern networks and cloud capabilities, data can connect previously siloed operations.

With a shaky data foundation, however, the potential for innovation in government is capped. That potential is also untapped though, as the sheer amount and quality of data that government possesses presents an opportunity that has not yet been explored.



## Tips for IT



- New projects should center on data and its usability.
- Ensure that systems are in place to scrub, store and process data, as analytics can make the incorporation of new technologies easier and alleviate intractable difficulties with older ones.

That's why the recently released Federal Data Strategy, including sets of best practices and principles for data governance for the nation's government, was a monumental step forward for agencies. By standardizing the practices and principles that agencies use to evaluate their data, and formalizing an action plan for agencies to take control of their data, the federal government can unlock new capabilities with the use of data.

Best practices are already in use by some agencies. Scientific communities, such as the National Oceanic and Atmospheric Administration (NOAA), NASA and the National Weather Service (NWS), are well-versed in best practices for the sharing and usage of data. Learning from them, these policies now just need to be spread throughout the rest of government.

Two of the most important best practices require agencies to share data between levels of government and formalize standards for the filing and classification of data.

Furthermore, open data laws are forcing agencies to publish more public data in accessible and usable forms online. With that will come good news, in the form of civilian efforts using public data to build projects that the federal government can glean insight from and take advantage of. Zielinski said that he had encouraged his son, who's interested in math and science, to use data.gov as the source for a school project.

Mandates from above will help ensure agencies take their data seriously, but internal culture shifts will have to occur to use data to its full potential. Therefore, agencies need to plan for the future with investments in data quality and the systems surrounding it.



# Bringing Emerging Technologies to Life to Empower the Workforce

Emerging technologies and their role in IT modernization can seem abstract for many employees. After all, artificial intelligence and blockchain aren't visible outside of code and front-facing portals, but their impact on the way people work has been profound.

Other emerging technologies, however, are quite tangible by themselves. Driverless cars and drone technologies are entering the fold, and they're already changing society. And government is responsible for it all.

"Folks do want to start leveraging these new and emerging technologies," Zielinski said.

Blockchain and RPA have gained popularity at GSA, and more is to come. GSA often serves as a testing ground for technology programs in government because of its mission to, as Zielinski described, serve the missions of all of the other federal agencies. Similarly, blockchain at HHS, McFarland said, has galvanized employees with the right training.

Across government, however, there are several barriers to incorporating emerging technologies. As previous sections have discussed, data and culture can preclude helpful technologies from ever gaining a foothold within agencies. Just as crucially, however, agencies often don't feel like one emerging technology would accomplish the goal of the roundtable – holistically modernizing IT. If the emerging technology failed to integrate with other systems or improve business processes, the business case might not justify an expensive upgrade for a very siloed impact.

"I haven't met an agency yet where their mission is building infrastructure," Lefrancois, Verizon's public sector CTO, said.

Cloud technologies, which come in a variety of accessible forms, can help solve these challenges. Through the cloud, data can be shared between departments and agencies easily, as systems housed off-premises can transcend physical barriers between offices. Edge computing power is also gained by users, who are enabled to work with mobility and modern devices.

The business case is also self-explanatory. Cloud providers launch cloud applications and capabilities that agencies can immediately put into place, allowing for front-facing results that can be adjusted with Agile processes.

## Tips for End Users



- If advocating for emerging technologies, emphasize the business case.
- The reality of federal work is that many systems are aging and that some solutions will lag years behind the private sector in adoption. If solutions make financial sense, however, governments will have more reason to push for them.

“It gives you that flexibility to try things, and not necessarily wait for a six- to nine-month procurement cycle and when it shows up, you forgot what you wanted in the first place,” Baker said.

Cloud enhances emerging technologies, including blockchain, AI, driverless cars and drones. In fact, many of their systems depend on the benefits of the cloud – data ubiquity, agility and mobility.

As modern employees clamor for their experiences in the private sector to be extended to their work in the public sector, agencies need to carefully consider their approach to emerging technologies. Many different pieces of emerging technology would fit into place and help employees do their jobs, but because of organizational constraints, piecemeal solutions won’t do the trick.

Instead, agencies need to focus on improving centrally to welcome in expansive, widely impactful emerging technologies that have immense business value, such as blockchain at HHS or RPA at GSA. By improving the accessibility of data, preparing front-end results and readying employees for modern capabilities, agencies can ensure they’re ready for the cloud.

“This is really bringing the CIO shop closer to the mission,” Lefrancois said.



# Setting Aside Security Fears to Focus on Upgrading Systems

Few business elements in government have to move more quickly than security. Threats are always ramping up, and governments need to buttress their defense. Considering the accelerating pace of attacks and threats, however, it may be surprising that attendees of the roundtable agreed: Security is not the danger it once was from the systems side.

That's good news, since security has often stifled procurement and leadership from acquiring solutions that would truly modernize systems and transform the workforce. While a possible solution might have seemed effective at performing its role, security checks could expose it to months of testing before the solution itself could be purchased.

Worse, security could either find gaps or fail to prove that the solution was secure fitting in with existing systems and data. And in federal government, acquisition always errs on the safe side.

Fortunately, federal programs have shored up the safety of vendor solutions and agency practices. Compelling agencies to monitor their networks, the Continuous Diagnostics and Mitigation (CDM) program requires that agencies achieve four security capabilities by improving their cybersecurity posture, reducing the number of attack surfaces, increasing visibility and expediting reporting. The four capabilities are monitoring and reporting what is on the network, who is on the network, what is happening on the network and, finally, how data is being protected.

The Federal Risk and Authorization Management Program (FedRAMP), meanwhile, bolsters security from a vendor side while accelerating the time with which agencies can acquire cloud solutions. Cloud providers have to go through strenuous security checks to ensure they're authorized to work with federal agencies in the cloud. Permits cover security clearances, depending on what data would be housed in the cloud, but even the Defense Department (DoD) has FedRAMP high-authorized solutions.

"We've really gotten past a lot of security and compliance issues that people were sort of struggling with five or six years ago," Baker said.

AWS clouds are certified for high-impact levels of FedRAMP and can also help agencies with architectures that are ready for the Trusted Internet Connections (TIC) program, which aims to lower the number of network boundary connections on federal networks.



Through programs like these, the federal government has moved to a modern state of security. But that's not to say cybersecurity isn't still a priority for governments everywhere.

Governments have adopted a focus on securing networks and data, as opposed to trying to lock down all devices, which have increased dramatically in number in recent years. As a result, solutions are generally secure, but users' information is the new prize for attackers, as they can use it to access systems. Popular forms of attacks, such as phishing and malware, work through users.

Cybersecurity initiatives are in place to identify insider threats and train employees on how to protect their agencies. These programs and the awareness of how data and networks lead security concerns have changed the way that agencies set up systems.

Because of FedRAMP and similar state and local government programs, agencies are generally safe using cloud solutions and further buying emerging technologies. More so, the biggest security threats to systems can come through legacy technologies, which might not have to undergo stringent new programs and checks while constantly requiring maintenance to crucial components, a small federal agency employee warned.

## Tips for Security



- Changes in security are happening all the time, and the TIC 3.0 initiative soon will formalize a plan to allow for more emerging technologies.
- While federal programs advance to allow for the safe incorporation of new solutions, evaluate the risks of legacy technologies and train employees on how to keep data safe.



---

# How AWS and Verizon Can Help

In partnership, AWS and Verizon are bringing accessible cloud capabilities to agencies. Using AWS cloud, agencies can deploy modern applications quickly outside of procurement processes, immediately offering employees the opportunity to work with their preferred devices on efficient and modern tools.

AWS cloud is easily accessible and scalable, and answers all questions of federal clearance. As agencies increasingly go to edge computing models and IoT devices join federal networks, security and speed are imperative. Verizon Secure Cloud Interconnect (SCI) offers private connections to the cloud that are secure while enabling the full range of cloud mobility and capabilities. With SCI, new clouds can be added quickly and scaled automatically.

“As the scale of these cloud services continue to grow, the cost efficiencies are going to continue to get better and better and better,” Baker said.

Speed will increase as well, with 5G playing host to another set of edge computing devices. As agencies adopt modern workflows and need the utmost secure data-sharing, cloud computing through Verizon and AWS offers the flexibility and ease of use to elevate government missions.

“As you start looking at software-based services, everything now can be put into a services model, and those can be very disruptive to the organization. But you have to be very forward-thinking about it – not what you have, but what do you want to have?” Lefrancois said.

*Learn more about [Verizon](#).*

*Learn more about [AWS](#).*



---

## Conclusion

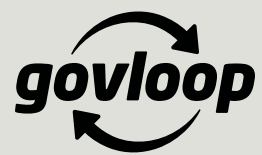
In government, IT modernization is a process of emotions as much as technology. While tech capabilities look good on paper, change is a frightening phenomenon for many involved in federal offices. In order to achieve true holistic IT modernization, security, leadership, acquisitions, user and IT teams need to be able to come together with an understood vision of how they want their organization to look.

Every employee plays their part in shedding legacy IT and welcoming business-friendly systems. Remember these tips on your way to modernization:

- Innovators should start small on projects, but think about bigger impacts, stoking support from members of different departments.
- Leaders need a clear and decisive direction, but they also still need to engage and consider the opinions of affected parties.
- IT employees need to be adaptable, working with users and acquisitions to make change happen, while identifying data as a focus.
- End users need to embrace a mentality of change and advocate for the technologies they want to see by making a business case to leaders.
- Security teams need to comprehensively consider risks, weighing the dangers of legacy systems and making use of governmentwide programs to evaluate newer ones.

Services like those provided by AWS and Verizon can help. In addition to increasing the rapidity of service, they meet and exceed governmentwide security standards and offer immediate return on investment for all parties. With engagement and training, emerging technologies and cloud capabilities can be brought in to help employees launch novel and impactful projects that will directly assist agencies in accomplishing their missions.





1152 15th St. NW Suite 800  
Washington, DC 20005

P (202) 407-7421 | F (202) 407-7501  
[www.govloop.com](http://www.govloop.com)  
[@GovLoop](https://twitter.com/GovLoop)