



# Best Practices for Supporting a Modern, Hybrid Workforce

# Introduction

---

How do you prepare for a future that's full of uncertainties and unforeseen variables? Governments have grappled with that question for ages, but this time feels different.

They're planning for a future where modern and resilient agencies must ensure that the business of government can withstand disruptions, whether natural or manmade. Plus, many employees aren't working exclusively in an office, which has prompted new ways of securing networks and access to systems and data.

**So how can agencies be nimble and rethink what modern means in the context of their operations?** Preparing for the unexpected is key. This means ensuring that secure, accessible and equitable services are at the core of how agencies operate. These capabilities must be ubiquitous for employees and the constituents they serve.

In this resource, we explore how a modernization mindset is shaping every facet of government operations, from digital services to improving cybersecurity and delivering services to customers. A billion-dollar funding infusion from the federal COVID-19 relief bill could accelerate many of these efforts in new ways.

You'll glean insights from public servants at NASA, the U.S. Army Corps of Engineers and the Homeland Security Department. They first shared their best practices and case studies during a recent GovLoop virtual event, which you can watch in full using the link below. Read on for key takeaways and best practices for cultivating a modernization mindset at your agency.

[Watch the on-demand session](#)

## The experts who participated in the virtual event are:

**Margaret Brisbane**, CIO and Director of the Information Technology Department, Miami-Dade County, Florida

**Robert Leahy**, Chief Information Officer and Director of Information Technology and Communications Division, NASA Goddard Space Flight Center

**Robert Dorr**, Acting Executive Director, Business Management Directorate, Office of the Chief Information Officer, Homeland Security Department

**Jose Arvelo**, Senior Director, FED Systems Engineering, Citrix

**Ken Liska**, Senior Director, SLG Systems Engineering, Citrix

**Linzie Oliver**, Chief, Governance and Architecture Division, U.S. Army Corps of Engineers

# In the News: Government Modernization Efforts at a Glance

---

## **The American Rescue Plan Act of 2021**

Signed into law on March 11, the \$1.9 trillion economic package includes \$350 billion for state, local, territorial and tribal governments to support equitable economic recovery, and \$10 billion for those entities to help with capital projects such as broadband infrastructure.

## **Technology Modernization Fund (TMF)**

Housed at the General Services Administration (GSA), the TMF is a centralized pool of money loaned out in parcels to government agencies for capital improvement tech projects. Though established in 2017 with the Modernizing Government Technology Act, the TMF has since found it difficult to find a foothold within the larger budgeting discussions, receiving scant payments.

That was the case until recently when the American Rescue Plan passed, injecting stimulus across the country and depositing \$1 billion into TMF coffers. The TMF Board will give cybersecurity projects priority consideration, as announced by GSA and the Office of Management and Budget (OMB). The funding also comes with greater flexibility for how the money is distributed to agencies and repaid.

## **FedRAMP**

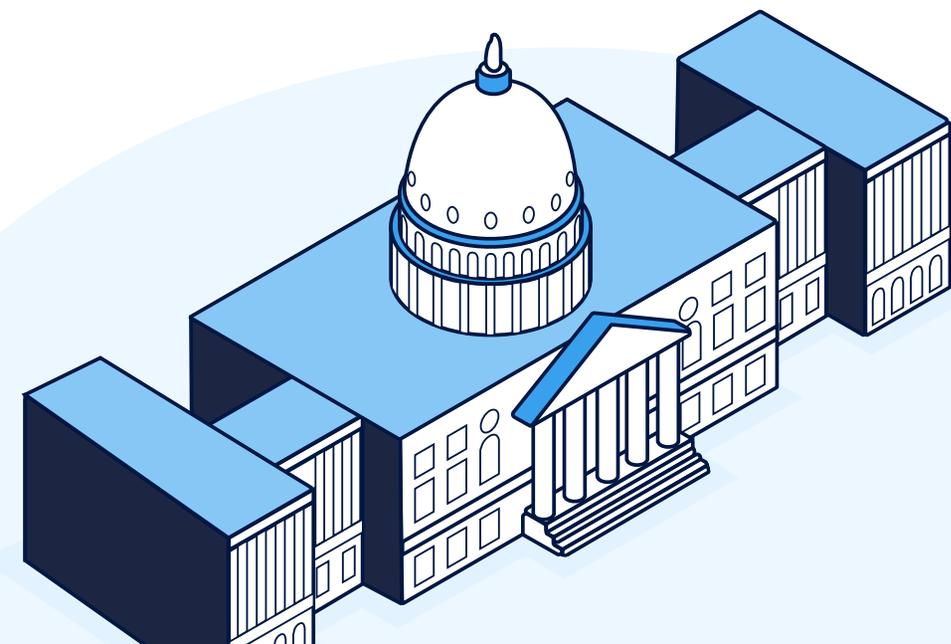
Since 2011, the Federal Risk and Authorization Management Program (FedRAMP) has authorized which cloud products and services can host federal data. Tapping into FedRAMP's cloud security standards, the Biden administration made the program one of its cybersecurity Executive Order's (EO) biggest stars.

- **No. 1 among the EO's FedRAMP priorities is developing a governmentwide strategy for federal cloud security.** Before debuting, this strategy will try ensuring agencies broadly understand the risks from cloud-based services and how to effectively address them.
- **Ranking second among the EO's FedRAMP goals is a technical reference documenting secure cloud architecture.** Once released, this resource will illustrate recommended approaches to cloud migration and data collection, protection and reporting for agencies.
- **Lastly, the EO charges FedRAMP with identifying the cloud services and protections available to agencies based on incident severity.** This framework will also list the data and processing activities associated with these services and protections.

## **StateRAMP**

StateRAMP is a nonprofit organization that certifies cloud solutions that meet basic cybersecurity standards for holding state and local data. The group is modeled after FedRAMP.

- StateRAMP launched in **January 2021**. The idea for the group was first conceived in **February 2020**.
- StateRAMP membership officially opened for state and local government officials and cloud providers in **April 2021**.



# Your Roadmap for Meeting the Cyber Executive Order

A conversation with  
Linzie Oliver



Shoring up government cybersecurity falls into the category of easier said than done, despite a heavy emphasis due to the recent bombardment of attacks. In fact, that easier-said-than-done tag follows many government mandates and presidential prescriptions, which often carry zero congressional funding.

The recent Biden [Executive Order](#), however, strikes a different tone – for one, because of its urgency, and for another, because of its backing.

Though not directly funded by any congressional dollars, Biden’s Executive Order on Improving the Nation’s Cybersecurity trails a watershed funding surge for the Technology Modernization Fund. Housed at the GSA, the TMF is a centralized pool of money loaned out in parcels to government agencies for capital improvement tech projects.

“Many of our capabilities within government are antiquated, and they just don’t address our security needs today,” said Linzie Oliver, Chief of the Governance and Architecture Division within the U.S. Army Corps of Engineers.

The vision for the TMF is that with millions of dollars available outside the usual budget, agencies can replace and upgrade ingrained and underlying technology systems that are outdated.

Though established in 2017 with the Modernizing Government Technology Act, the TMF has since struggled to find a foothold within the larger budgeting discussions, receiving scant payments. That was the case until recently when the American Rescue Plan Act passed, injecting stimulus across the country and depositing \$1 billion into TMF coffers. The TMF Board will give cybersecurity projects priority consideration, as announced by GSA and the Office of Management and Budget.

Following an application and award process, TMF funds are used for modernization projects of all stripes – mainframes, contact centers, cloud and more.

But Oliver suggests that cybersecurity is an overarching top priority for all of government, and even projects that are not security-focused still must put protection up front.

“You can turn on the news today and see all the issues going on with security,” Oliver said. “This fund allows you to ... strengthen security posture much faster than you would before.”

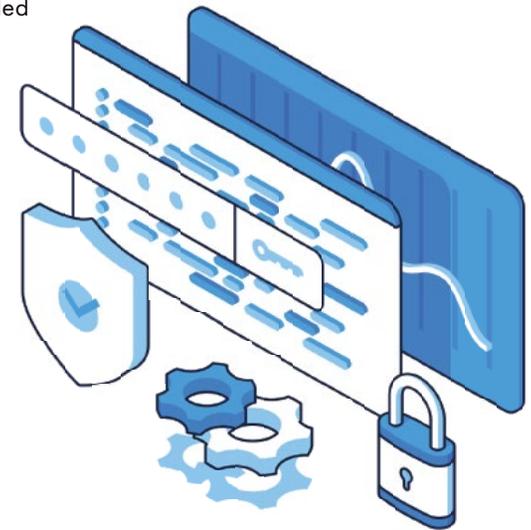
The Army Corps of Engineers works to meet unique standards. Composed of civilian and military employees and working with numerous agencies, the Army Corps of Engineers adheres to both Defense Department and OMB cybersecurity mandates, Oliver said.

With continuous revisions to cybersecurity posture, such as the Biden EO’s tilt toward zero-trust security philosophies, Oliver said agencies must be able to monitor their systems and know what they have – and what they don’t. Modernization to cloud technologies can remove impediments to enterprise visibility.

Oliver also encouraged agencies to have a plan and engage stakeholders. He commended his agency’s Chief Information Officer, Dovarius Peoples, for establishing a clear plan within 90 days of coming onboard.

With those priorities in mind, the U.S. Army Corps of Engineers continues to move to a modern, secure enterprise.

“Cybersecurity is No. 1 for us. It tops our list. It’s No. 1. It’s No. 2. It’s No. 3,” Oliver said.



# How to Think About the Cloud in New Ways

A conversation with  
**Jose Arvelo** and  
**Ken Liska**



Cloud experts often talk about the value of going after low-hanging fruit – that is, fairly simple cloud deployments that provide clear and quick benefits. But the lowest-hanging fruit is not necessarily the sweetest.

During the pandemic, cloud delivered a clear return on investment for many agencies, helping them to make a hard pivot to remote work. But rather than stop there, agencies should use 2020 as a starting point for using the cloud to drive their modernization efforts, according to two subject matter experts from Citrix, which provides secure cloud-based digital workspace technology.

Here are four ways that agencies can reach beyond the low-hanging fruit and see even greater benefits, especially as they move into a hybrid work environment.

## 1. Think About Your Customer

Never mind the metrics that go into various reports. You need to look beyond the IT team and hear from the people who are using the services you provide, said Jose Arvelo, Senior Director of Federal Sales Engineering Manager at Citrix.

“Understand how your services really are affecting or supporting the mission, and make sure that as you go forward, you target the IT services that are going to provide the most value,” he said.

## 2. Think About User Experience From the Inside Out

For as long as agencies have supported remote workers, those workers typically have had to accept a lower quality of IT services. Whether they were working on the road or from home, those services wouldn’t be the same as if they were in the office.

That’s got to change, said Ken Liska, Systems Engineering Manager for Citrix State and Local Government Team. “When you have a hybrid workforce, you need to make sure the user experience is just as good for the employees that are remote as are in person,” he said.

In fact, cloud and virtualization make it possible to provide an even better experience, since digital workspace technology is based on server-grade hardware, rather outdated desktop technology, Liska said.

## 3. Think About Security From the Inside Out

In the same way, agencies need to provide one set of security measures for employees working in the office and another, more stringent set for remote workers.

Given how the hybrid work environment inevitably blurs the distinction between internal and external workers, it’s better to assume that everyone could be an attacker, and every device could be vulnerable, said Liska.

Such an approach — essentially, a zero-trust approach — also means that the agency can protect all users with a common set of products and solutions, he said.

## 4. Think About Security Plus Context

Cyber experts often joke that the best way to secure a device is to stick it in a locked drawer. From an employee’s perspective, on the other hand, that’s not a winning option. In fact, the employee’s perspective is what’s often missing from security discussions, said Arvelo.

When thinking about security in the hybrid workplace, start by thinking about the context in which employees will be working — not just the device or devices they use but where they will be working and the work they will be doing.

“Whenever we approach this sort of conversation, we always start from the end user and work our way toward the technical outcome, what the technical solution should look like,” Arvelo said.

**During GovLoop’s panel discussion on cloud, we asked attendees the following: *Is your agency investing more in cloud in 2021 than in previous years?***



# Maximizing Your Agency's Modernization With Cloud

A conversation with  
Margaret Brisbane,  
Robert Leahy and  
Robert Dorr



No one wants to fall behind the times, and governments are no exception. Unfortunately, many agencies are finding they cannot provide the same quality as today's top companies. Unlike the private sector's best businesses, much of the public sector is neither modern nor provides an enjoyable customer experience (CX).

Cloud computing may be the answer. The cloud offers computer system resources like data storage on demand; gradually, the result is faster, more flexible agencies. Using cloud to modernize their products and services, agencies can deliver more pleasing CX to their employees and constituents more quickly.

So why are some agencies struggling to adopt the cloud? Although beneficial, embracing the cloud is not as simple as flicking a switch. Cloud adoption is not only about modernizing technology; it is about modernizing people and processes too.

Here are three ways agencies can successfully modernize their operations using cloud and recent federal funding prompted by the COVID-19 pandemic.

## 1. Standardize the User Experience

Modernization may require agencies to provide the same user experience (UX) to both their employees and their constituents. Nowadays, both parties may use the same public sector offerings either in person or digitally.

"It is not one size fits all," said Margaret Brisbane, CIO and Director of the Information Technology Department of Miami-Dade County, Florida, of UX. "We need to ensure all their experiences are similar and they can be productive."

Standardizing UX with the cloud provides more consistent, satisfying encounters between agencies' products and services and the people using them.

## 2. Strengthen Security

Agencies cannot forget security during modernization, or they may jeopardize their sensitive citizen data. Security is thus the cornerstone of any successful cloud adoption.

"It's on the top of everybody's list," said Robert Leahy, Chief Information Officer and the Director of the Information Technology and Communications Division at the National Aeronautics and Space Administration's Goddard Space Flight Center. "A big part of modernization is making sure what we do is safe and secure."

Agencies that do not consider security during modernization may suffer costly disruptions that damage public trust in their work.

## 3. Make Modernization Relatable

People sometimes resist change if they do not understand its benefits. As a result, explaining why modernization efforts such as cloud adoption are valuable can make these ventures successful.

"We can sometimes get bogged down in IT speak," said Robert Dorr, Executive Director of the Homeland Security Department's Business Management Directorate in the Office of the Chief Information Officer. "How does this impact the organization's mission and its customers?"

Addressing that question for an agency's leaders can generate the goodwill needed to get modernization efforts like cloud migration off the ground.

## The Last Word

Change management can become a major barrier to modernization, Brisbane said. For example, she cited how Miami-Dade County recently helped its workforce adjust to a new cloud-based enterprise resource planning (ERP) platform.

"There is quite a lot of education we do here on any change in technology," she said. "Having people very engaged in the change is essential."

## How Citrix Helps

Citrix provides workspace technology that is designed to deliver a frictionless employee experience — with a common set of capabilities and a consistent look and feel across any device and from any location.

But that frictionless experience cannot come at the expense of security. Citrix provides secure access solutions that take a zero-trust approach to security. Unlike a traditional on-premises virtual private network, Citrix solutions provide granular access to both software-as-a-service and internal web apps, without needing to give them access to the full network, as often happens with a virtual private network-based solution.

# Takeaways

## 10 Tips for Creating a Culture of Modernization

- 1. Provide a consistent user experience.** Whether employees are working in the office, at home or on the road, they should be able to log on and start working without missing a beat.
- 2. Adopt a common set of security capabilities.** In a hybrid work environment, the line between internal and external users is hopelessly blurred. Assume everyone is a potential threat (i.e., go zero trust).
- 3. Learn from your experiences.** To prepare for hybrid work, use 2020 as an “evaluation year,” fixing what didn’t work and building on what did.
- 4. Invest in services, not hardware.** As one expert said, “Friends don’t let friends build new data centers.”
- 5. Put security first.** Even non-security projects should have security at the forefront. When in conjunction with a plan, this will vastly improve your organization’s outlook.
- 6. Establish priorities.** Create a roadmap for your organization and follow it. Look for funding opportunities and bring teams and stakeholders together to accomplish overarching goals.
- 7. Know your audience.** When you are talking about IT modernization, make sure you discuss it in a way that makes sense to the people you are trying to reach. For example, explaining the budget mechanics of adopting cloud computing could make the technology more appealing to auditors.
- 8. Make convenient products and services for constituents.** This includes mobile-friendly services that are accessible via smartphones, and self-service options.
- 9. Practice accountability and transparency.** Constituents expect clarity around how government products and services are reaching them and how their tax dollars are being spent.
- 10. Increase agencywide resilience.** Modernization efforts will not matter if they do not factor potential disturbances such as severe weather into the equation. New tools should thus help your agency respond to, recover from and continuously operate during disturbances.



### About Citrix

Citrix provides technology that empowers organizations to #UnlockPotential & deliver a better employee experience. Our goal is to give people the space to succeed & do their best work - wherever they are.

Our platform brings intelligence, virtualization, workspace and app delivery, a zero-trust security approach, and data analytics together into a seamless experience that fosters innovation, resilience, and business continuity. From enabling sustainable remote work models to streamlining the journey to multi-cloud, Citrix helps securely deliver how work gets done today and in the future.

Learn more at [www.citrix.com/government](http://www.citrix.com/government).



### About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).

[www.govloop.com](http://www.govloop.com) | [@GovLoop](https://twitter.com/GovLoop)