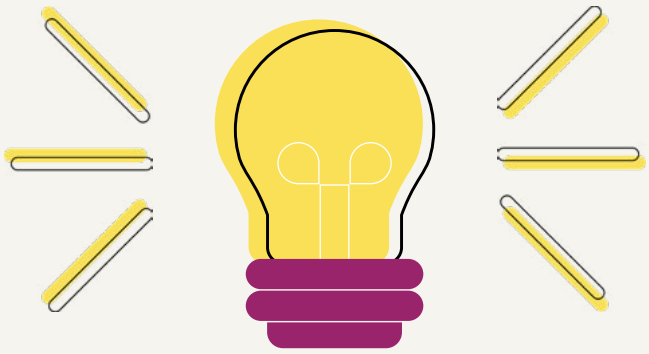
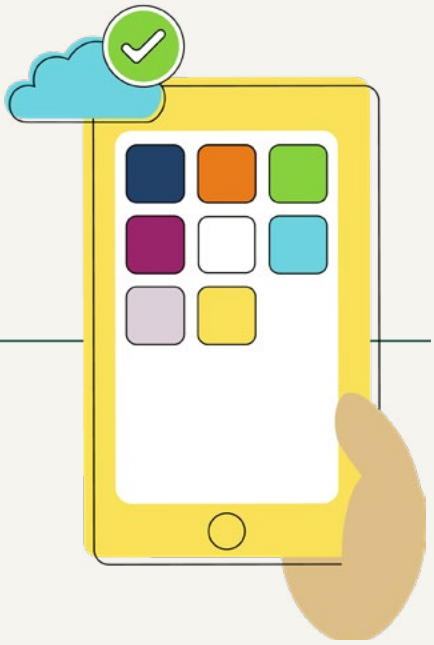
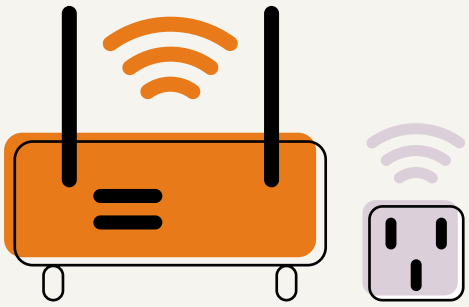
# Technology Transformation Strategies:



## From Idea

## to Implementation





govloop

# CONTENTS

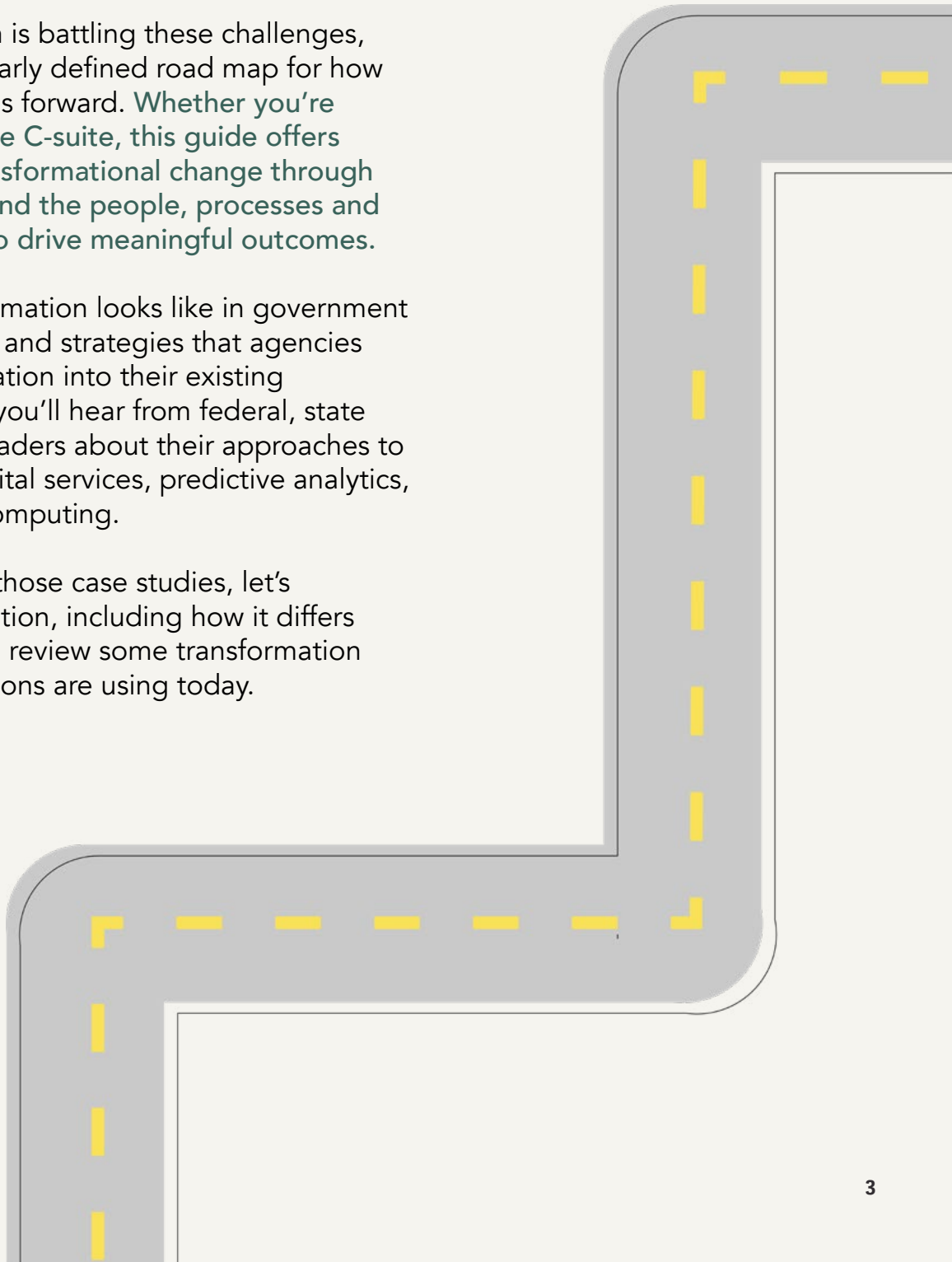
# EXECUTIVE SUMMARY

Transformation is a loaded word that holds both tremendous promise and a level of uncertainty, particularly for those charting the course from ideation to tangible results. This is especially true in government, where the road to transformation can be fraught with false starts, bureaucracy, changing priorities and a lack of clarity around mission outcomes.

Maybe your organization is battling these challenges, or maybe you have a clearly defined road map for how you will move good ideas forward. Whether you're on the frontlines or in the C-suite, this guide offers an insightful look at transformational change through the lens of technology and the people, processes and collaboration required to drive meaningful outcomes.

You'll learn what transformation looks like in government today, and the key steps and strategies that agencies are using to inject innovation into their existing operations. Specifically, you'll hear from federal, state and local government leaders about their approaches to transformation using digital services, predictive analytics, zero trust, 5G and fog computing.

But before we dive into those case studies, let's clearly define transformation, including how it differs from modernization, and review some transformation strategies that organizations are using today.



# Transformation vs. Modernization: What's the difference?

Transformation and modernization are commonplace in the government's IT vocabulary, but they carry different objectives, goals and outcomes depending on whom you ask. Modernization focuses on updating legacy technology, usually the infrastructure or IT backbone that supports an agency, whether it be networks, servers or operating systems. Transformation, on the other hand, is about improving operating outcomes or changing the way an agency empowers employees, serves customers and does business.

For this guide, GovLoop is using this working definition: Transformation sits at the intersection of IT modernization and innovation and enables agencies to implement impactful wins that create better, more dynamic services.

Transformation isn't a one-time event. It's incremental, iterative and supported by IT modernization.

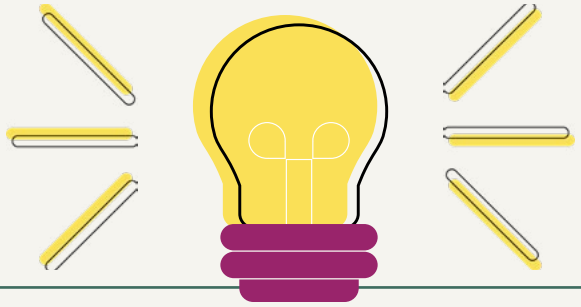
You'll often see the word "digital" precede transformation because moving from manual, cumbersome operations to online and mobile-friendly features can drastically change the way employees work and the public's interactions with the government.

But what does transformation actually look like? From an IT perspective, it could mean shifting from the model of owning and operating technology in a government facility or data center to outsourcing to the cloud, said G. Nagesh Rao, Director of Business Intelligence Technology Solutions (BiTS) in the Small Business Administration's (SBA) Office of the Chief Information Officer. It's not so much the cloud itself that's transformational but rather how agencies can use it to enhance services. Modernization, by comparison, would entail upgrading from Windows 7 to Windows 10, for example, Rao said.

Although we are discussing transformation through the lens of technology, transformation isn't about a shiny new object or a complete overhaul that takes years to execute. Lynn Overmann, a former Obama administration Senior Adviser to the U.S. Chief Technology Officer (CTO), warned against the urge to throw technology at every problem:


Although technology is an enabler, true transformation is only as solid and lasting as the processes, policies and workforce buy-in supporting it.

# From the Experts:



Technology transformation applies modern methodologies and technologies to improve the lives of citizens and public servants. It's about making services more accessible, efficient, and effective with modern applications, platforms, processes, personnel and software solutions.

— Adapted from the General Services Administration's (GSA) Technology Transformation Services

"Caterpillar becomes a butterfly, that's transformation. Butterfly augmenting itself in the environment that it's in so that it can be more effective to evade predators, that's modernization."

— G. Nagesh Rao, Director of BiTS, SBA's Office of the Chief Information Officer

IT modernization governmentwide is focused on upgrading legacy systems and building a more modern and secure architecture for government IT systems. Agencies have attempted to modernize their systems but have been stymied by a variety of factors, including resource prioritization, ability to procure services quickly and technical issues.

— Adapted from the Report to the President on Federal IT Modernization

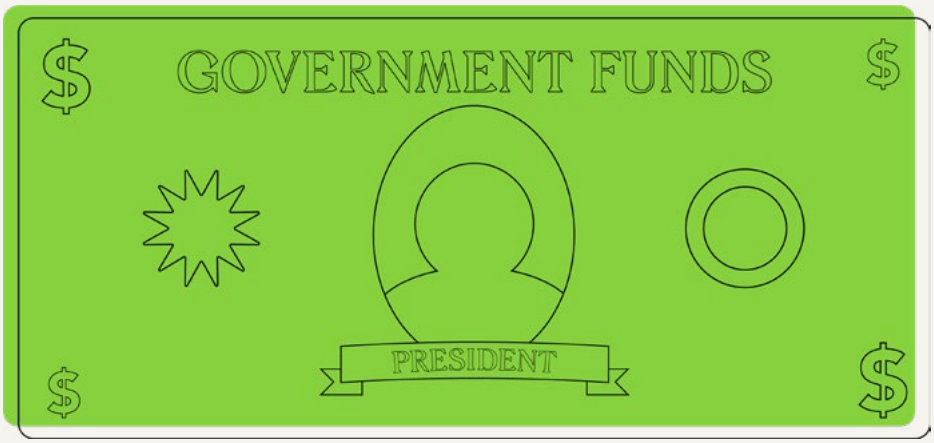
"When I think of operationalizing those words [modernization and transformation], I don't think of it necessarily in an IT context. But for me modernization would mean more of the deployment of the technology, and the transformation…has to do with the people side of things in terms of how we are using the technology."

— Sarah Twose, Program Analyst, Diplomatic Innovation Division, Office of eDiplomacy, State Department

# SNAPSHOT OF GOVERNMENT & INDUSTRY STRATEGIES

Many models and approaches exist for taking transformational ideas, implementing them and then scaling them. The General Services Administration's (GSA) 10x program has a model it uses to fund, support and develop ideas from federal employees. Those ideas focus on how technology can improve the public's experience with the government, and 10x funds each idea in phases.

Below we've outlined the 10x project phases – and their dollar amounts – as a guide for developing a transformation framework to scale good ideas. If you already have a framework in place, compare and contrast it to these phases.




## 10x Project Ideas

### Identify a Problem

Point to the pain. We start by gathering ideas from federal civil servants. These proposals are intentionally short — only about two to three sentences — to stay focused on a specific, concrete problem. If your idea is selected, 10x will notify you and will hire a small team for Phase 1 to further evaluate the idea.

### Phase 1: Investigation — $20,000

Think it through. Spend two to three weeks exploring the accepted idea to define what it would take to be successful — uncovering risks, roadblocks and opportunities. At this point, people who submit ideas can act as subject-matter experts for a research and strategy team dedicated to quickly evaluating the idea. Only the most promising ideas will proceed into Phase 2.

## Phase 2: Discovery — $175,000

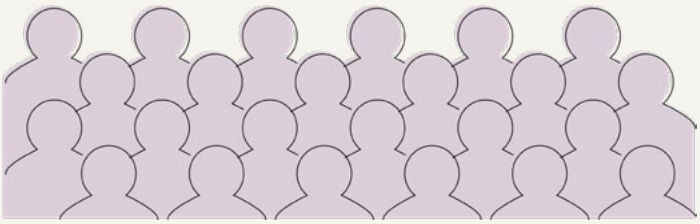
Go deep. Gain a detailed understanding about the industry, problem, market fit, finances, timeline, regulatory environment and how to scale. Analyze what could go right and wrong, and create an initial strategy to address these issues. For this and later phases, you are welcome to work alongside the team that is developing this idea.

## Phase 3: Development — $500,000

Build it out and plan for the future. Develop a functional minimum viable product with at least one active customer. Create a product roadmap tied to a customer acquisition strategy. Provide a data-backed market analysis. Estimate the cost and effort required to continue sustainably building and maintaining the product long term.

## Phase 4: Scale — Up to $1.28 million

Bring the product or service to the largest possible audience.

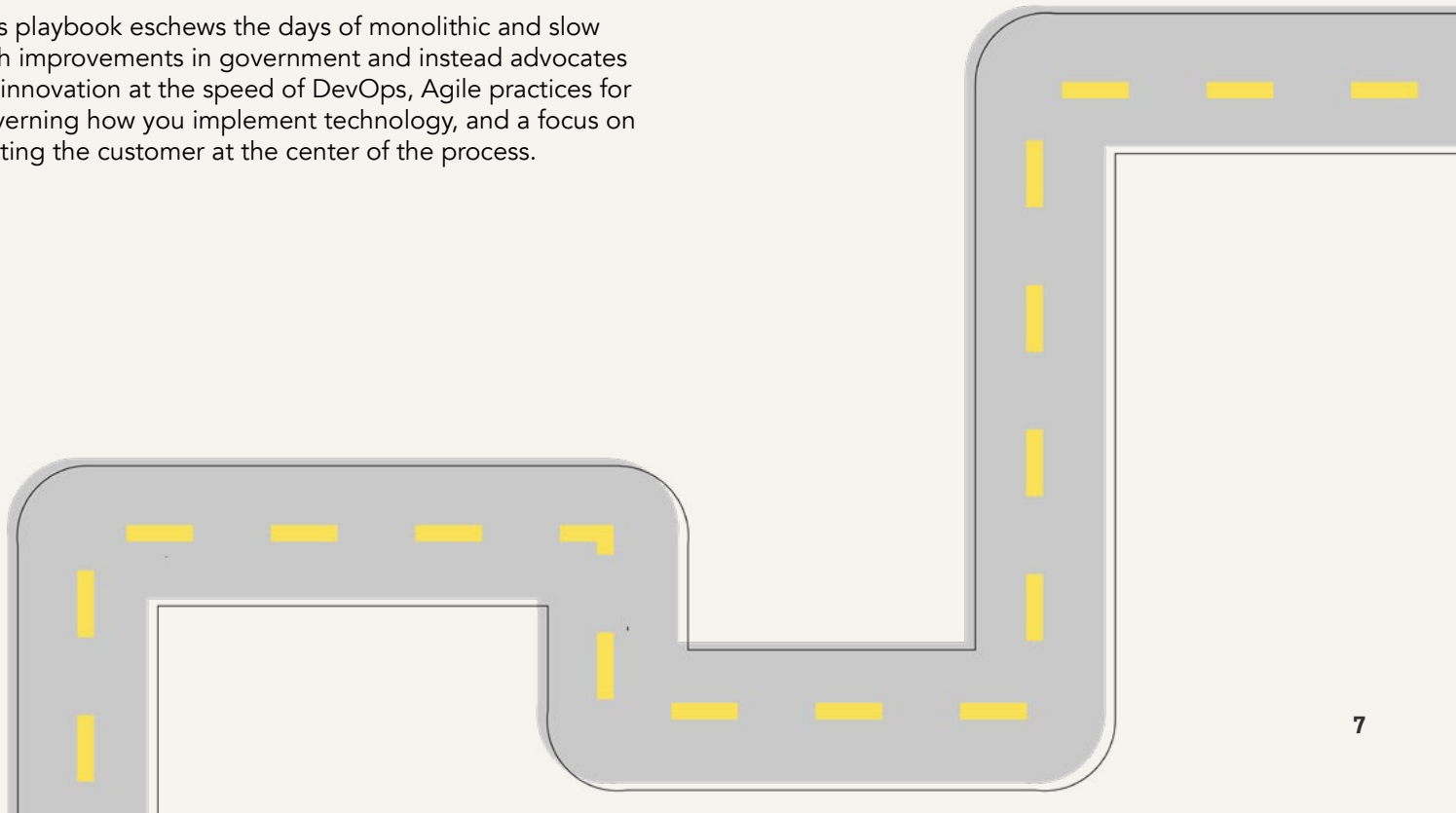


# IT Transformation Playbook

There's no shortage of playbooks for how to transform your organization using IT. Forrester's IT Transformation Playbook, for example, provides a roadmap for addressing the underlying governance, people and processes required to deliver transformation.

This playbook eschews the days of monolithic and slow tech improvements in government and instead advocates for innovation at the speed of DevOps, Agile practices for governing how you implement technology, and a focus on putting the customer at the center of the process.

To better understand what transformation looks like from ideation to implementation, we highlight specific examples and practical tips in the following pages to help you on your journey.



## Industry Spotlight

# 3 PRIORITIES FOR DATA-DRIVEN TRANSFORMATION

*An interview with Daniel Lee, Solutions Architect, Red Hat*

Government agencies are beginning their transformation journeys to bring value to their customers. They need real-time insights that inform real-time actions, whether they're responding to cyber intrusions, making medical decisions or managing logistics operations. Agencies need the ability to adjust their services to their consumers' needs in days or minutes — not months.

"But they often have so many policy hurdles, and their processes are very complex," said Daniel Lee, Solutions Architect at Red Hat, an open-source software solutions provider. "These can act as barriers in their transformation journey."

These barriers create a ripple effect, leaving agencies hamstrung in their efforts to efficiently collect, analyze and act on massive heterogeneous data — from text to multimedia to logs and more. With massive data serving as the backbone for transformation, agencies need a strategy for extracting value out of their most critical asset.

Lee highlighted three key areas that agencies must prioritize to support data-driven transformation:

1. **Data governance.** Every organization must lay down a data governance strategy that allows them to ensure proper handling of data while maintaining high standards for data quality and security. Laying down these policies and procedures first provides a foundation that can drive the agility needed when it comes time to developing data analytic initiatives.

2. **Artificial intelligence/machine learning with a zero trust security mindset.** AI/ML is one of the fastest growing government IT initiatives, and a zero trust security model can provide the proper protection. This model starts with the raw data and does not stop until the resulting analytic outcomes. "For government agencies, security always starts with data," Lee said. The reliability of the resulting AI/ML insights will depend on the security efforts that revolve around the entire software supply chain cycle.

3. **Technology platform.** The workflow for AI/ML involves a plethora of activities, which involves very complex processes and procedures. This is where it is critical to have a platform, such as Red Hat OpenShift Container Platform, that can support agencies' workflows end-to-end and allow them to focus on delivering business results through their data analytics. For example, by mapping data governance requirements to the platform, it allows complex organizational policies and procedures, such as access control policies, to be supported through technology for scenarios that involve multiple data classification levels.

"It's not about the technologies alone," Lee said. "When you couple transformative technologies such as OpenShift with process and culture improvements, agencies will see holistic changes," Lee said.

Culturally speaking, one of the misconceptions that must be addressed is that security is detrimental to efficiency. Rather, incorporating security from the start can enhance operations and help agencies accelerate their work by avoiding pitfalls that cause longer delays.

**"If agencies follow these best practices, they'll have real-time insights that allow them to make real-time actions, rather than always reacting," Lee said. "It's going to allow them to respond much quicker, even proactively many times, while heightening their security posture."**

## Transformation Strategy for

# DIGITAL SERVICES

Investments in digital services have become a staple for governments of all sizes seeking to make antiquated operations more user-friendly and efficient. For the Defense Department's (DoD) internal digital SWAT team, this was especially true as it overhauled the outdated system that hundreds of thousands of service members rely on to manage permanent and temporary relocations.

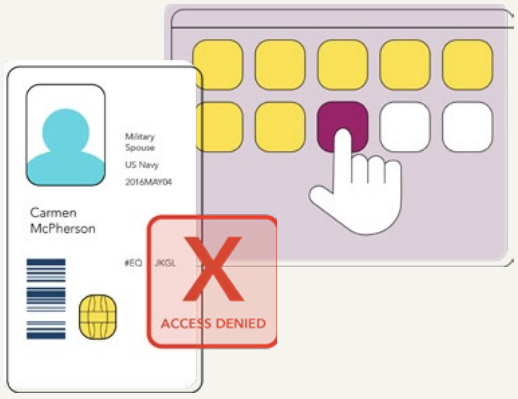
**Challenge:**

## Managing Complex Military Moves With an Antiquated System

Each year, nearly 425,000 service members and their families undergo the permanent change of station process, or longer-term assignments that require them to move to a different part of the country or world. The bulk of those moves — roughly 180,000 — occurs in a three-month period between June 1 and Sept. 1.

The Defense Personal Property System (DPS), which DoD uses to manage these moves, was technically challenged, said Jeff Clark, Digital Service Expert at Defense Digital Service (DDS). "It was meant to manage the process, not to help the service member," Clark said, and uptime was unreliable.

Exacerbating the issue was the fact that spouses of service members couldn't log in to the system and coordinate moving plans. Only service members were authorized to log in, and they had to use their government credential, or Common Access Card (CAC).




**Solution:**

## Overhaul the System and User Experience

U.S. Transportation Command, which facilitates DoD's relationship with moving companies and storage providers for household goods, reached out to DDS for help.

DDS partnered with the command to replace the old system with a new solution that eases the burden and stress for military personnel who are reassigned to new duty locations.

A big component of the discovery sprint, or the process for understanding stakeholders' pain paints, involved gathering service members and their spouses in a room to walk the DDS team through their experiences and share what capabilities they wish they had at their disposal, said Katie Olson, DDS Chief of Staff.

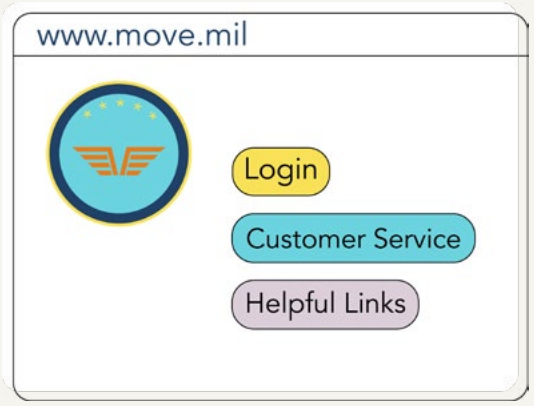
Using that feedback, DDS rebuilt Move.mil, the informational website for service members' moves. The DDS team also initiated the system's replacement with a mobile-friendly web application called MilMove, which allows military personnel and their families to log their orders and plan for their upcoming moves.

As part of the transformational process, DDS led an Other Transaction Authority (OTA) contract. DoD sometimes uses OTAs, which are generally exempt from federal procurement laws and regulations, to develop prototypes and contract for follow-on production of a successful prototype project. In this case, an OTA enabled the team to continue working with the software firm Truss to expand the prototye, said Clark, who served as Product Manager for MilMove.

The team also brought in an all-women user experience (UX) design shop called Sliced Bread out of Silicon Valley to help them take a user-centered approach to transformation. That meant engaging with and documenting how users responded to system improvements.

Roughly five months after DDS kicked off the project, it delivered a minimum viable product. As is the case with DDS projects, the team transitioned MilMove back to the command in September 2019 for continued development and expansion.

Military branches rolling out MilMove include the Air Force first, followed by the Marine Corps and the Army.




## Outcome:
## Seamless, Secure and Faster Online Process

Among the benefits that the new system and capabilities provides are ease of use and speed, Clark said. Using DPS, it took over an hour just for users to log in. The first service members to test MilMove did it in less than 30 minutes. Using an iterative process to tweak user experience, the team then offered a mobile version that allowed service members to upload their permanent change of station orders to the system using their phone cameras. The overall process decreased to about five minutes for simple moves.

The DDS team used login.gov, the government's authentication and identity proofing platform, to make online interactions with MilMove simpler and more intuitive. Instead of using a CAC to confirm who they were before logging in, service members received a login.gov account that they could use across multiple government systems to prove their identity.

"One of the other pieces of it, which I think is important… [is] sometimes our projects do lead to policy changes," Olson said. For instance, now spouses can log in to book movers, coordinate insurance and complete other tasks.

For DDS, the ultimate goal is not just creating prototypes or new products, but also changing policies that permeate the department and improve lives, Olson said.

## From Idea to Implementation:
## Charting a Path to Digital Services

Here are practical steps from DDS for implementing and collaborating on digital services.

**Determine the criteria for selecting digital services projects.** At DDS, that includes potential impact, reusability, sustainability and appetite for long-term ownership of the project within the department.

**Design with users, not for users.** Work closely with leaders — from the secretary's office down — to identify priority needs and challenges.

**Use discovery sprints or immersive learning to connect with users.** Go where the work is being done and meet with users to identify pain points and determine what matters most to them.

**Have a procurement plan in place.** For example, DDS has waiver authority that allows the team to use vetted private-sector tools to solve some of DoD's biggest tech problems.

**Think about scale and reuse early and often.** The goal shouldn't be to create one-off projects that work for a single office or group. When possible, look for opportunities to scale to other parts of the organization facing similar pain points.

## Transformation Strategy for

# PREDICTIVE ANALYTICS

Predictive analytics provides the likelihood of the future based on the past, and government agencies such as the Defense Logistics Agency (DLA) have recently begun to use this technology to optimize operations. Efforts don't have to be large to see transformational effects, but they start with a good foundation in data.

**Challenge:**

## The Sheer Amount of Data

Data has become ubiquitous and prominent in people's lives. Online stores recommend products based on purchase history; streaming services recommend shows after one unfortunate binge-watch. Whether the data history is good or bad, representative or unrepresentative of you, this is what predictive analytics does — makes predictions about the future based on the past.

The past, therefore, is critical to successful analytics. The quality of the data that an analytics project is based on — whether it's descriptive, diagnostic or predictive — is the key and the challenge that agencies face when it comes to adopting analytics. Today, decisions are increasingly made with data in mind, from improving digital experiences for users to clearing the snow for residents to getting supplies to U.S. warfighters worldwide, which is DLA's responsibility and mission.

"A challenge we had — and we still face — is just the sheer amount of data we have," said Teresa Smith, Chief Data Officer (CDO) at DLA. The troves of data that the agency collects and the lack of structure to manage it made it difficult to determine whether the data was clean or authoritative enough to use in analyses for optimizing the supply-chain processes for warfighters.

**Solution:**

## Good Governance for Advanced Analytics

The CDO role has been pivotal for managing better data quality. The establishment of the office and position at DLA three years ago has encouraged a better data foundation by providing governance, the formal management of data as an asset. The structure has also allowed for more advanced analytics, such as predictive analytics, to take place.

Predictive analytics goes a step beyond showing why something happened by presenting what might happen in the future — or "what-if analytics," Smith said. For DLA, it's a helpful tool when it comes to filling orders for certain resources, including rations and equipment, for DoD personnel around the world.

"Like any organization, we have a finite budget, and so we want to make sure that we're maximizing the return for the warfighter and providing them optimum readiness," Smith said.

To do so, the agency built a material availability predictor model that shows a forecast of demand for materials up to a year in the future. It has helped the agency look at the holistic picture of its portfolio to glean insight for what actions best fit the future.

"We can look in the rearview mirror and see what [material availability] has been, what it is today and what it's projected to be," Smith said.

## Outcome:
# Satisfied Employees

Currently, material availability metrics at the agency are at record-high. But it's not entirely due to the technology. "It's probably largely because of the hard work of the folks," Smith said.

What predictive analytics has done, even in a small use case, is enable employees to anticipate problems and raise proactive solutions.

"Nobody likes to work constantly with their hair on fire," Smith said.

This has brought more value to their jobs and led to more innovative solutions. Responding reactively often leads to resolving issues in the same way as before, which isn't necessarily the best way. Predictive analytics allows more time for employees to develop creative solutions and get ahead of the problem. Essentially, if deployed well, the technology can add time, value and money to an operation.

"That's the beauty of it," Smith said. "We're not going to catch every problem, but it does inform us ahead of time."


## From Idea to Implementation:
# A Recipe for Predictive Analytics Success

Here are the steps Smith suggests agencies take to successfully start using predictive analytics:

**Gather good ingredients.** You need to make sure your data is clean, quality data. "If you have bad data, you're going to make bad decisions," Smith said. She emphasized that analytics starts with quality data, which is data that comes from an authoritative source and has not been manipulated. In other words, you want clean, organic ingredients. If you can verify that the data comes straight from the system source, it's likely to be of better quality.

**Actually, good enough ingredients.** At the same time, Smith urges agencies to not be paralyzed about perfect data mining. Move forward with what you have. It should be "roughly right" or directionally right. "At some point, if it's good enough, let's go forward," Smith said. "But you have to have good enough data to move forward."

**Enlist the sous chefs.** Gather the right people to make the secret sauce. With the right data, you need to bring in the right people — preferably, those with tech savvy who can work with the data and those with operational savvy can understand how it fits in with operations. The partnership can then build the appropriate formulas, visualization and so on — "the secret sauce behind the predictions" — to unlock the fullest and most relevant value of predictive analytics in agency operations.

**Obtain head chef support.** Make sure you have executive buy-in. In the same vein as gathering the right people, having leadership sponsor and support the funds and manpower to stand up predictive analytics efforts is important. Like many new investments and transformational efforts, support from the top will help agencywide understanding about an initiative and signal its worth.

"There has to be an agreed-upon recognition that this is something that we need to do, and we're not just spending resources," Smith said.

## Transformation Strategy for

# ZERO TRUST

Cybersecurity is due for a paradigm change. Many organizations continue to rely on traditional perimeter-based security measures, even though they know that cloud, mobility and related technologies have rendered the perimeter far more porous than they would like – and their network assets far more vulnerable.

The Air Force is in the vanguard of major organizations that are looking to something called zero trust architecture. GovLoop sat down with William Marion, the service's Deputy Chief Information Officer (CIO), to learn more about its strategy.

### Challenge:
## Good Security in an Era of Increased Complexity

Like many organizations, the Air Force has responded to the growing complexity of the IT environment by adding layer upon layer of security. Cyber experts talk about security measures as "walled gardens" designed to keep assets safe from intruders.

The problem is that the Air Force IT enterprise is larger and more complex than that of most organizations: Operations stretch from one part of the globe to another, and data and applications cross multiple types of networks. Ideally, the service wants to create an end-to-end secure enterprise, because cyberspace is contested space. "It's a wicked scale problem," Marion said.

The traditional solution? Build more walled gardens. Unfortunately, with the complexity of the environment, any given transaction, such as retrieving data, needs to pass through multiple walled gardens and checkpoints, which translates into a big hit on performance. UX "is intolerable," he said. Something else is needed.

### Solution:
## A Zero Trust Architecture

An analyst at Forrester Research was the first to articulate the concept of a zero trust architecture in 2010, but the notion is not new. As long as agencies have been adding encryption and other security measures to mobile devices, they have been taking a zero trust-like approach.

Traditional perimeter-based security is the equivalent of having a security guard at the front of your office building and requiring everyone to show an ID card to enter. If that is the only entrance, you might be safe to assume that everyone in your office has permission to be there – that is, security cleared them to be there. That's perimeter-based security.

But what if you add multiple entrances to the building, so many, in fact, it's no longer practical to rely on guards? At that point, you need to lock individual offices and systems with a security fob system, with each person's fob configured to access only the resources they need for their jobs. That's zero-trust security.

The goal is to apply security controls within the network itself, locking down individual datasets, applications and systems. That's the model that the Air Force is adopting.

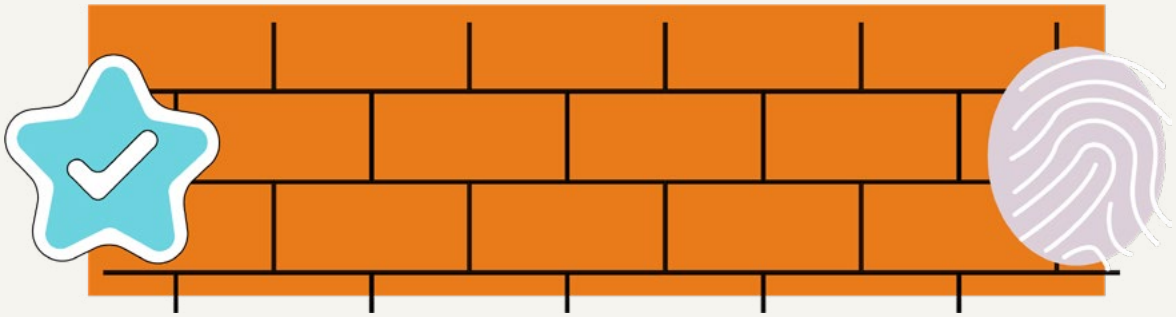
## Outcome:
# Better Security, Better UX

As always, when Air Force leaders think about outcomes, they think in terms of mission. Given that cyber is contested space, strong security is essential. But so is a good UX. If airmen and airwomen on the flight line are unable to access the information that they need at mission speed, that's a problem.

By putting controls in place at the application and data levels, a zero trust approach should improve overall security and reduce the need for walled gardens – which should improve UX. That's not to say that the Air Force will cease to defend the perimeter. But the perimeter will no longer be the last line of defense.

Zero trust is part of a much broader effort to change how the Air Force approaches IT. In the past year, the service has piloted different components of its vision of Enterprise-IT-as-a-Service, in which it will rely on contractors to deliver core commercial IT services. Another program, called Cloud Hosted Enterprise Services, delivers email, calendaring and virtual collaboration tools worldwide through the cloud-based Microsoft Office 365.

Zero trust represents a big change, but it's a necessary one, Marion said. "We've got to continue to pivot to zero trust. We've got to challenge the status quo," he said.



## From Idea to Implementation:
# A Path to Zero Trust

When it comes to taking a new approach to solving problems, one of the biggest challenges is getting buy-in from the various stakeholders. Without it, institutional resistance is bound to stop a new idea in its tracks. Here is a look at how the concept of zero trust has gained traction in the Air Force.

**Executive buy-in.** In any organization, senior leaders are unlikely to adopt a new approach at a conceptual level. What they want to know is: How will zero trust address our pain points? Because zero trust offers a way to solve longstanding problems related to UX, service leaders were not hard to convince. It also helped that senior leaders saw that major IT companies have taken this same path.

**Mission leader buy-in.** The next step is to get buy-in from those who are leading key mission areas. Here, you need to talk about zero trust in terms of mission imperative. In the case of the Air Force, Marion's goal is to enable airmen and -women to be as productive on the flight line as they are at their desks. That's the kind of vision that Air Force commanders can get behind, and they have.

**Broader organizational buy-in.** With end users, one of the best ways to get buy-in is to frame zero trust in terms of more familiar applications. For example, anyone banking online recognizes the value of requiring two-factor authentication with every transaction – not just a user ID but also a nother identifier, such as a biometric – even if the network is supposed to be secure. That's a good way to begin a conversation about zero trust.

# Transformation Strategy for 5G

The futuristic world that movies foretold hinges on a new faster, broad-spectrum wireless network. Autonomous vehicles, drone delivery and remote medical procedures can be carried out only with 5G. But as 5G rolls out, security concerns roll in. This time, the Cybersecurity and Infrastructure Security Agency (CISA) is one step ahead in protecting its prized assets.

## Challenge:
## Into the Unknown

5G is coming. It's inevitable. And in many ways, it's already here.

The fifth generation of wireless technology that will transform telecommunications networks has every sector of the U.S. frantically preparing for its widespread adoption. The faster, federated 5G network will enable possibilities unachievable until now, such as truly autonomous cars on roadways, package-delivering drones and increasingly realistic virtual and augmented reality, using all parts of the spectrum.

Because it exists as a wireless network, 5G will soon usher nearly every smartphone user into the movement.

If all of that sounds like good news, that's because it is. The challenge arises in the wider attack surface that results from increased mobility and more devices.

CISA, part of the Homeland Security Department (DHS), has carried the flag for network security in the U.S.. Although widespread use of 5G is not expected for another two to three years, CISA is preparing for how to protect assets in an increasingly remote and network-driven security environment.

Cyberattacks are only increasing in number, and soon, they will have more targets. Attacks on 5G-enabled systems could be catastrophic – the compromise of drones or autonomous vehicles could endanger public safety. Before 5G hits the market fully, the U.S. government is readying its people, policies and systems.

## Solution:
## Building Before Launch

No single solution exists for 5G security. As is the case across the federal government, modern security philosophies emphasize "safe, not sorry" authentication and authorization, permitting users access to only the systems they need while constantly verifying identity.

Zero trust is one such approach, a cybersecurity strategy that emphasizes security where users are as opposed to where data is stored. But that's not what will explicitly prevent cyberattacks from penetrating 5G's broadened range of devices.

CISA Assistant Director Bill Kolasky told GovLoop that 5G is just another evolving technology, and it is a product of an environment of big data and mobility. Kolasky, who leads the National Risk Management Center (NRMC), which works to identify and manage the nation's top threats, emphasized that standards, regulation and collaboration would help guide 5G's expansion in a way that did not carry significant risks to the U.S..

"We insist that we participate in the standards bodies," Kolasky said, noting that his team collaborates with industry on international boards and partnerships.

Fully rolling out 5G will also require that related systems catch up to the technology. Legacy systems that interact with or support 5G can present preventable vulnerabilities, so achieving a modern, software-secured network that can extend protections to networks' edges networks will be crucial.

Widespread 5G usage is not expected until 2022, meaning government has another few years to prepare — an important advantage over attackers.

## Outcome:
# A Model for Emerging Tech Security

Although 5G already exists in select locations such as big cities and stadiums, overall, the federal government is ahead of the game.

CISA revealed an unclassified and public version of its risk overview for 5G in late July 2019, forecasting what government and industry need to do to prepare for the nascent technology. The International Telecommunication Union (ITU) and 3rd Generation Partnership Project (3GPP) are finalizing international standards. Industry and government are plotting out rural road maps for 5G.

Meanwhile, national and international companies, boards and governments are meeting to lay the preparatory groundwork for 5G.

Kolasky said that in many ways, the rollout to 5G has been a model for security. Although elements of 5G remain unpredictable, the stakeholders are filling potholes on the road to the next-generation wireless network – accounting for security and economic and technological impacts.

"One of my key points when I talk about this is we're having the 5G security conversation before the 5G network becomes a reality, rather than after it is," Kolasky said. "And I think that's important because we can shape the 5G network and deploy it securely."

Too often a new innovation is pushed to the market for the socioeconomic benefits, leaving security in the dust, he said. Then, teams like CISA have to react.

The buildup to 5G is different. Kolasky said that the 5G model could serve as an example for innovations going forward: Put security first, and everyone will be on the same page.

## From Idea to Implementation:
# Charting a Path to 5G

CISA's public document highlights several ways to manage and lessen the risks of 5G. These same approaches can apply to the adoption of other emerging technologies.

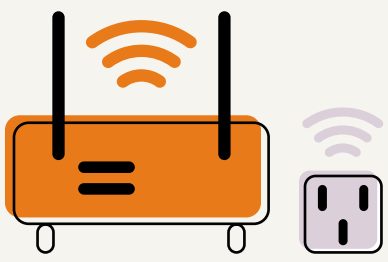
**Support the research and development of secure and trusted products**, much like how CISA is seeking out trusted partners in industry and joining them on advocacy and standardization boards. Doing so will eliminate risks of legacy system interoperability or unregulated development.

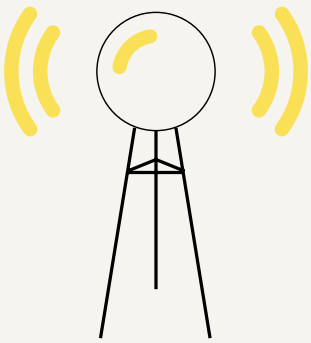
**Invest in other related technology sectors that will be affected so that adversaries cannot lead the way in the market.** For example, 5G will not only impact network providers but many cell phone manufacturers as well. All of these related communities need to be ready for 5G before its full, secure rollout.

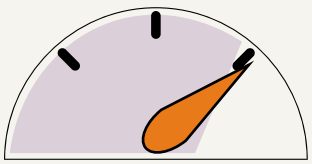
**Engage in standardization bodies such as ITU and 3GPP for 5G.** Establishing clear standards before the technology rolls out will lead to more manageable and visible technology.

**Ask companies where security efforts should focus and see where government can help fill gaps.** Many times, government bodies set the rules carefully to avoid the influence of big-money lobbyists and companies, but for emerging technologies, innovators need a seat at the table. Often, industry will have a better sense of potential vulnerabilities than government entities that are far removed from the development.

**Emphasize security across the network of related applications, services and possible users that will spring up from the new technology's marketplace.** In other words, consider the ripple effects. For example, autonomous vehicles are highly reliant on 5G technology, so CISA and other agencies are paying special attention to how that market will lean on 5G and what unique security vulnerabilities that poses.







## Transformation Strategy for

# FOG COMPUTING

Fog computing can transform agencies as it enables cloud on devices at the edge of their IT networks such as smartphones. Even better, fog computing is compatible with hybrid clouds, or the mix of publicly available cloud services with private environments such as on-premise IT that many agencies use.

**Challenge:**

## Sprawling IT

Mississippi CIO Craig Orgeron says that before the state adopted cloud computing, agencies were slowly disappearing under a mountain of IT. "We had significant infrastructure sprawl," Orgeron said. "We had lots of IT in many places."

He adds that physical IT was causing Mississippi's infrastructure sprawl. The resulting clutter made adopting new IT services harder for state agencies. "Data centers, server farms or older, mainframe technologies were the bread and butter of centralized IT for decades," he said. "And our governance model made it more difficult to put solutions in place."

Ultimately, the Department of Information Technology Services (ITS) embraced hybrid cloud to start clearing away Mississippi's overgrown IT. Orgeron notes that since embracing hybrid cloud, Mississippi has started delivering IT services statewide from one data center. "We're federated as a state," said Orgeron, who is also ITS' Executive Director. "We're not monolithic with all our IT people working under one roof. We're much more of a classic shared service organization."

Gradually, agencies such as ITS that reduce their physical IT save energy, funding and space that was previously spent maintaining it.

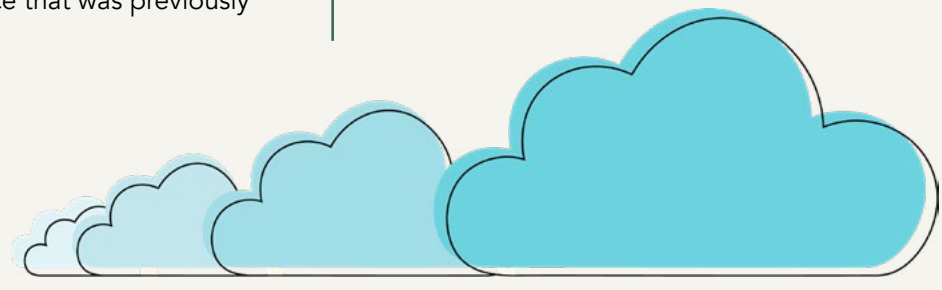
**Solution:**

## Extending IT's Reach With Hybrid Cloud

Hybrid cloud now allows scores of agencies across Mississippi to use IT services without building costly, dense physical infrastructure first. "With relatively nominal capital investments, we can set up an ecosystem that we believe goes a lot farther distance for IT that can be consumed," Orgeron said. "It's not just the statewide agencies, but the local governments, too. That's where the magic of consumable IT and compute services is a real sweet spot."

As Orgeron sees it, hybrid cloud has made ITS the broker for many of Mississippi's state and local agencies. By using cloud's scalability, ITS has managed to deliver convenient, reliable IT services such as computing power to agencies as they need them. "The scale is so great in cloud," he said. "You can't compete against it. Hybrid cloud made us able to offer a much more robust capacity. Convenience and reliability is a big one-two punch."

Even better, hybrid cloud now offers many of Mississippi's agencies a safety net for business continuity and natural disaster recovery. "You can do these things on a rolling, more flexible model," he said.

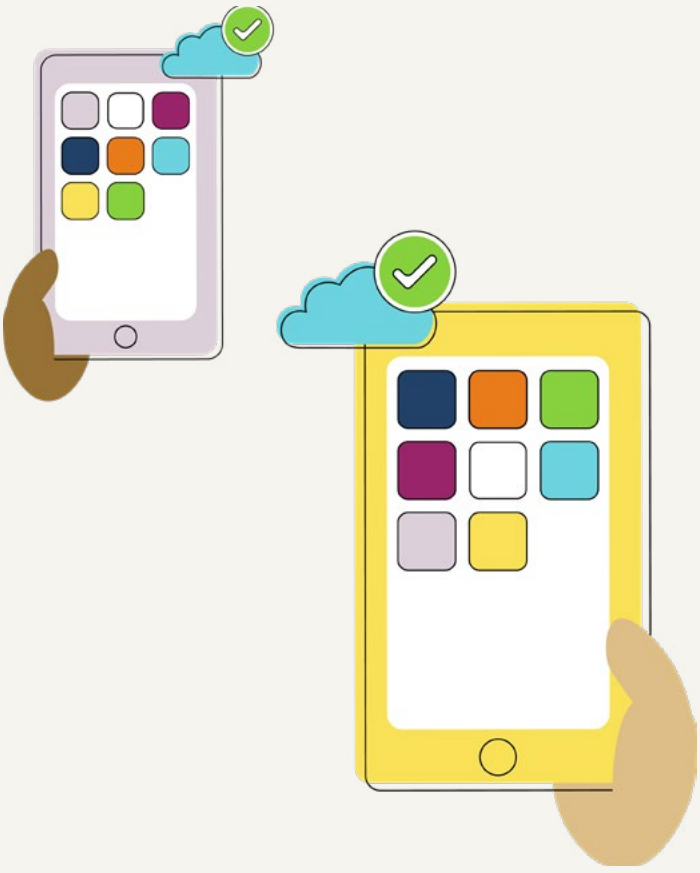


## Outcome:
# A Fog Computing Future

Where can agencies such as ITS head after deploying hybrid cloud? One possibility is fog computing, which extends cloud services past the edge of an agency's IT networks. Once past that point, fog computing enables cloud on edge devices such as smartphones and tablets. "There's some dipping our toe in the water," Orgeron said of Mississippi. "Fog computing is a blend of classic and edged-based cloud."

Although Mississippi doesn't have enterprise fog computing yet, Orgeron said it has major potential for the state. For example, it could help agencies deliver IT services from a central location to various Internet of Things (IoT) devices, which are tools that can connect via the internet and share data with one another. "You're gathering data of some kind or another at the edge," he said of IoT networks.

Orgeron estimates that Mississippi is several years away from broad fog computing, but hybrid cloud's far-reaching, on-demand services could eventually make it possible. "Consumable, commoditized technology is where it's at," he said.



## From Idea to Implementation:
# Charting a Path to Fog Computing

Per Mississippi's experience with hybrid cloud, Orgeron recommends the following steps for agencies looking to launch it with an eye toward fog computing at the edge of their networks:

**Map your cloud journey.** Orgeron says that agencies should consider how hybrid cloud will impact their operations, security and workforces. "I think we're at the tip of the iceberg in terms of workforce issues related to the skills to move to cloud," he said. "A lot of legacy technologies have to migrate one way or another." By considering these factors, Orgeron adds, agencies can avoid potential pitfalls during their cloud migration.

**Leverage cloud's consumption model.** Orgeron suggests that many agencies don't take full advantage of cloud's on-demand, subscription-based services. Agencies that fail to do so, he continues, may miss valuable financial savings. "It's pay as you go," he said. "It's commoditized to the nth degree. I may need twice as much computing power as I used today because it's the last day of the month and I'm running payroll."

Mississippi doesn't have one monolithic IT organization, so its cloud extends to several locations statewide. Regardless of where Mississippi's cloud is being used, it all emanates from the same centralized state data center, Orgeron said, adding that scenarios such as this can help other agencies decide how to best distribute cloud's capabilities for them.

**Revisit your agency's IT duties.** For many agencies, legacy IT means frequently maintaining and securing physical infrastructure to provide services to citizens and other external parties. Orgeron says that hybrid cloud changes this dynamic. "I foresee it impacting our capacity," he said of ITS. "I can see us using a much deeper and broader set of services. It will allow us to become the broker. That's going to be very significant in terms of our mission."

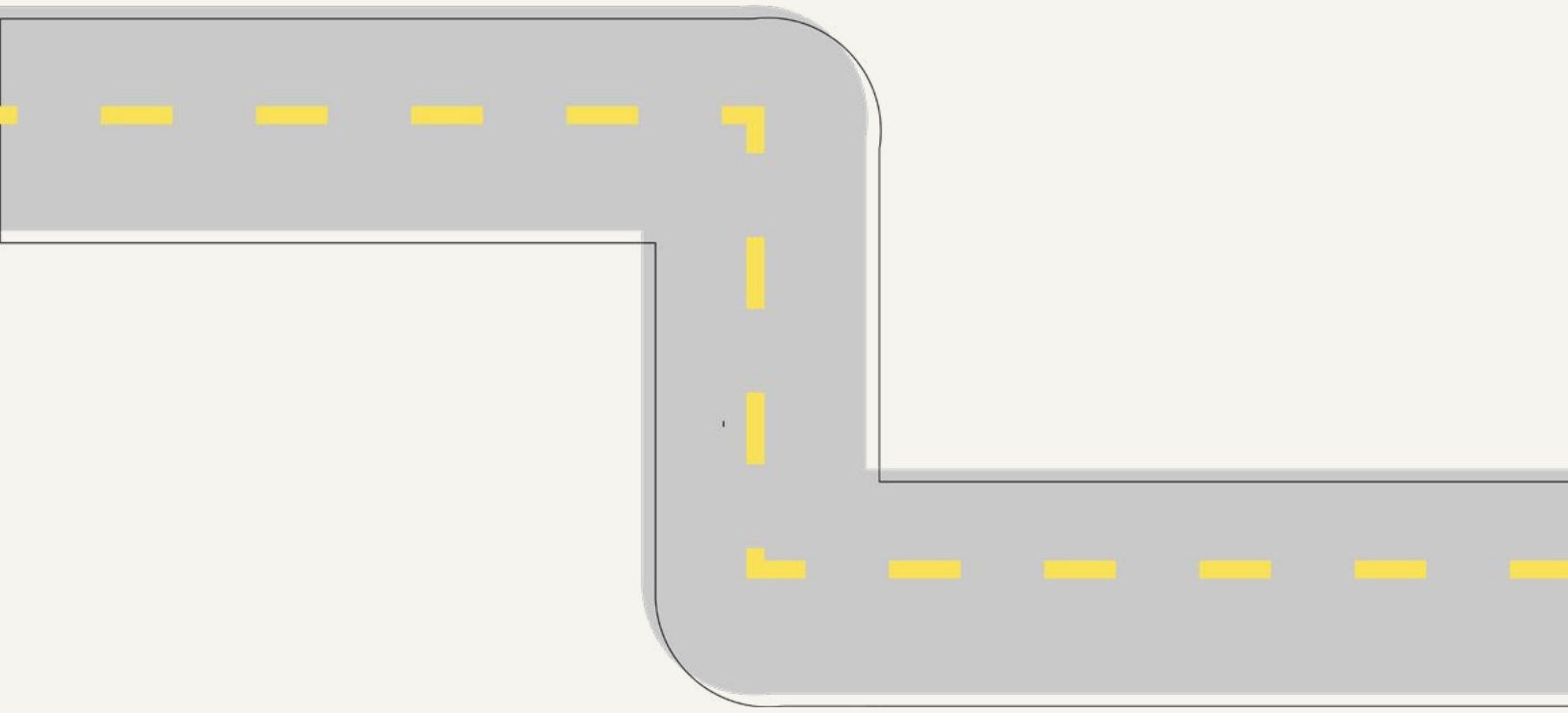
**Don't forget to centralize your IT.** Whether agencies use hybrid, fog or other clouds, Orgeron says agencies should view their IT as centralized to govern it. "Cloud or not, whether agencies are using the state data center or their office, I still think it's a centralized model," he said.

# CONCLUSION

The path to transforming operations looks different for every agency, depending on size, budget, mission and other factors. But common threads that must be at the forefront of any transformation change are: leadership support, clear goals and objectives, and a focus on meeting end users' needs.

When these foundations are in place, agencies can begin to consider how technology can support transformation. In other words, focus on coupling sound strategies with the right technologies to provide ongoing and iterative benefits for employees and external customers.

As you embark on or continue down the path to transformation, use this guide as an ongoing resource to review case studies and advice from others in government, explore new ideas and share effective approaches with decision-makers at your agency.



## 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.

govloop.com | @govloop

## Thank You

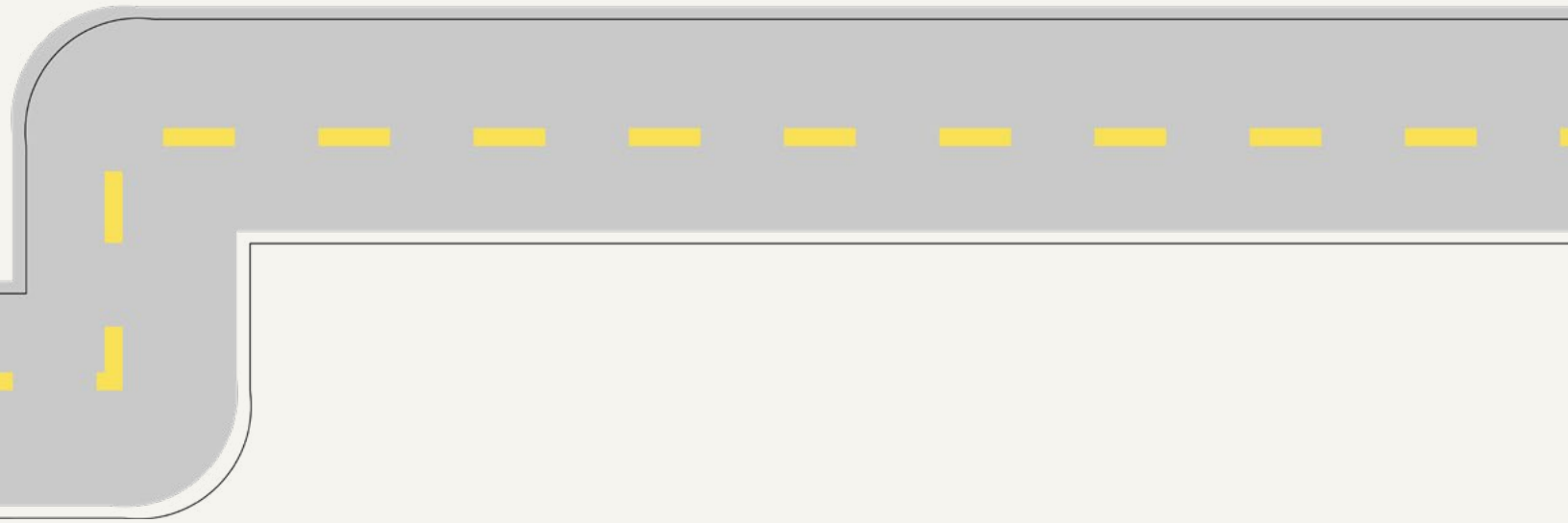
Thank you to RedHat for their support of this valuable resource for public sector professionals.

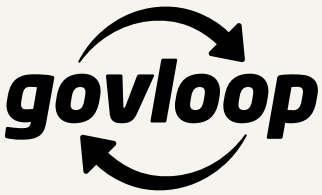
## Authors

Nicole Blake Johnson, Managing Editor
John Monroe, Content Director
Mark Hensch, Staff Writer
Isaac Constans, Staff Writer
Pearl Kim, Editorial Fellow

## Designer

Jacob Hege, Junior Graphic Designer





1152 15th St. NW Suite 800
Washington, DC 20005
P: (202) 407-7421
F: (202) 407-7501
www.govloop.com
@GovLoop