



CIO Perspectives: A New Vision for the Government Workplace

carahsoft



Contents

3	Introduction
4	Count on Carahsoft to Support Your COVID-19 Response Initiatives
6	Virtual Government at a Glance
9	Creating a Roadmap to Resilience
10	Is This the New Normal?
11	IT Gets the Spotlight
13	The Virtual Environment's Key Attributes
14	At GSA, the New Normal Is Not So New
17	Seeing Clearly With Network Visibility
18	What's Driving Your Modernization Strategy?
21	The 5 Elements of Government Digital Transformation
22	How Crisis Can Drive Innovation
25	Unified Endpoint Security: Bringing Order to Chaos
26	'In Every Crisis, There's Opportunity'
29	Identity Access Management in the Telework Era
30	Delaware's Path to Digital Service Delivery
33	Election Security Is About More Than Voting Machines
34	The Nuclear Regulatory Commission's Remote Work Success Story
37	How to Meet the IT Management Challenges of Remote Work
38	Best Practices
40	Conclusion: Is Resilience the New Normal?

Meet the Experts



Dorothy Aronson
CIO & Chief Data
Officer, NSF



Sylvia Burns
CIO of the Federal
Deposit Insurance
Corporation



James Collins
CIO, Delaware



Dave Nelson
CIO, NRC



David Shive
CIO, GSA



Theresa Szczurek
CIO & Executive Director
of OIT, Colorado

Carahsoft and GovLoop have partnered to provide this resource around the lessons learned by federal and state CIOs during the shift to telework to combat COVID-19. The goal is to guide government leaders and stakeholders interested in learning more about the latest strategies for teleworking and the solutions available to support these initiatives.

Introduction

In the early days of the COVID-19 crisis, most chief information officers (CIOs) focused on fundamental questions:

- How can agencies help employees stay productive and engaged when working at home and dealing with so many stresses and distractions?
- How can work processes be reengineered to work more effectively in a virtual environment?
- How can digital services help agencies support citizens when offices are closed?

Over time, however, they realized that in responding to the crisis, agencies were crafting a new model for agency operations. In many cases, it was indeed possible to carry out the business of agencies in a virtual environment. Employees could stay engaged, work processes often were streamlined and digital services proved their worth.

In part, the goal of this new model is to improve operational resiliency — ensuring that the next crisis, whether the next wave of COVID-19 or something entirely unexpected, is not nearly so disruptive.

But the new model also is geared toward transformation — helping agencies adopt more efficient and effective processes that deliver better services. Of course, this is what CIOs have envisioned for years.

This guide, created by GovLoop and Carahsoft, will explore how the COVID-19 crisis might reshape the future of government, drawing on the experiences and insights of government CIOs nationwide and the IT community's expertise. We also highlight some best practices around technology, policy and management strategies.

This might not be how we expected the future of government to arrive, but in responding to the challenges of this time, CIOs have the opportunity to help their agencies become more resilient and agile — ready to face whatever challenges the future might hold.







Count on Carahsoft® to Support Your COVID-19 Response Initiatives

Carahsoft's technology and reseller partners offer a range of solutions that enable telework across evolving mission needs and workflows. These solutions include productivity and collaboration platforms for keeping teams connected while working remotely; cybersecurity tools for securing communications across multiple networks and devices and combatting threats such as ransomware; virtual desktop infrastructure tools to allow for uninterrupted access to internal applications and data; and crisis communication and response tools to enable effective distribution of critical information to citizens and employees as new developments arise.







Telework & Collaboration Solutions

 Adobe Connect	 ATlassian	 aws partner network	 DELL Technologies	 Google Cloud	 MICRO FOCUS Government Solutions
 salesforce	 servicenow	 slack	 SpiderOak	 wire	 zoom

Crisis Communications & Response Solutions

 Acquia	 BlackBerry AtHoc	 Liferay	 qualtrics XM	 salesforce	 servicenow
--	--	---	--	--	--


Virtual Desktop Infrastructure (VDI) & Cloud Solutions

 aws partner network	 DELL Technologies	 Google Cloud	 Microsoft	 NUTANIX	 vmware
---	---	--	---	---	--

Productivity Tools

 Adobe	 Alfresco	 alteryx The Thrill of Solving	 CloudBees	 DELL Technologies	 DocuSign
 GitLab	 HashiCorp	 LinkedIn Learning	 MICRO FOCUS Government Solutions	 mongoDB	 NVIDIA
 Red Hat	 salesforce	 SAP	 servicenow	 smartsheet	 UiPath

Cybersecurity Solutions

Carahsoft's Telework & Distance Learning solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, NASPO ValuePoint, and numerous state and local contracts. To learn more, visit Carahsoft.com/Count-on-Carahsoft.

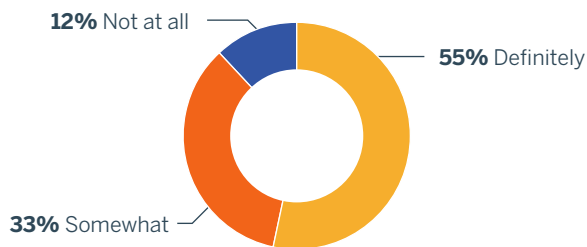
Virtual Government at a Glance

The Remote Work Learning Curve

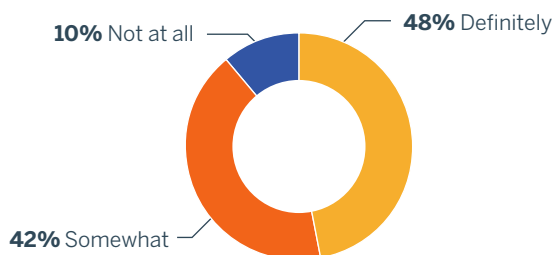
When agencies last wrote disaster recovery and business continuity plans they probably did not imagine a situation quite like COVID-19. In many cases, agencies have used their existing teleworking strategies as a starting point and scaled up for broad remote work. How has that approach played out?

In March 2020, GovLoop surveyed almost 700 federal, state and local government employees to find out. The results suggest that agencies have fared pretty well, although more work might need to be done before another crisis occurs. Here are three key data points:

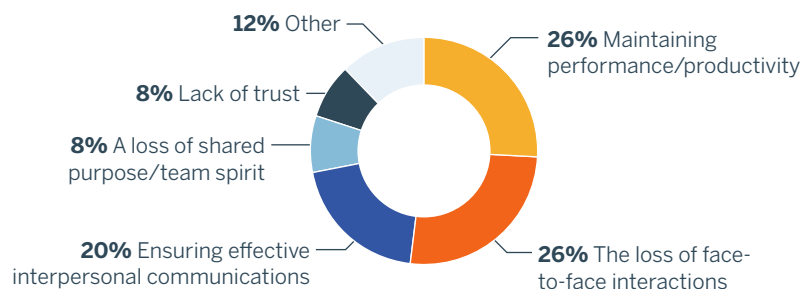
Are you confident that your supervisor can manage effectively in a virtual team environment?



Are you confident that your coworkers can work effectively in a virtual team environment?



What do you see as the biggest cultural challenge to working effectively in a team environment?



Remote Work, DoD-Style

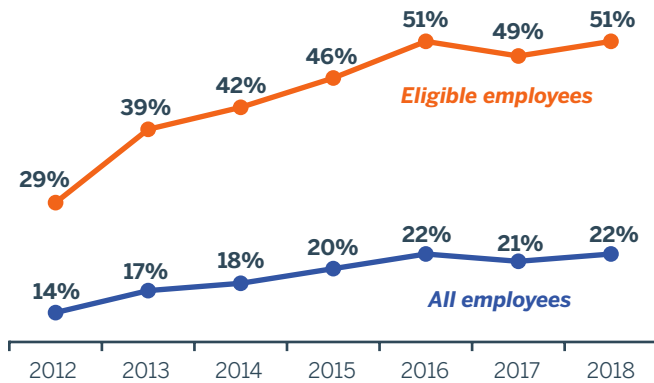
The Defense Department had to step up its support for remote workers significantly during the pandemic. Here are some of the numbers DoD CIO Dana Deasy shared during an April 13 press briefing:

- **2,000** Pentagon personnel received additional devices
- **65,000** additional Navy users are working remotely with mobile and desktop services
- The Defense Information Systems Agency/Joint Service Provider increased virtual internet service provider connections by **30%**
- DoD's telecom provider increased the department's current call volume capacity in the Pentagon by more than **50%**
- The Air Force has increased its bandwidth by more than **130%** by upgrading 12 key sites
- The Army has implemented measures that have led to a **400%** increase in data and voice capacity
- DoD has seen **tenfold growth** in global video services, Microsoft Outlook Web Access and enterprise audio conferencing

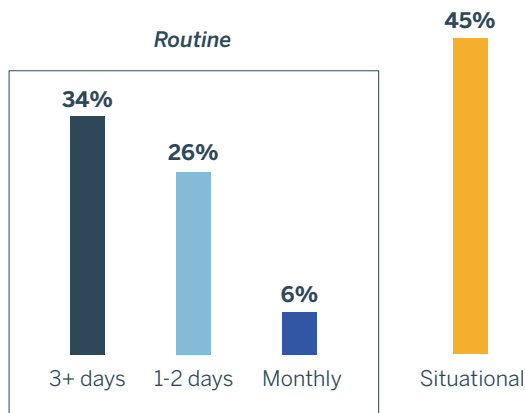
Telework Trending Upward

In its latest annual report to Congress, the Office of Personnel Management (OPM) notes that telework has leveled off in the past two years (through fiscal 2018) after several years of steady growth. Also, there continues to be a significant gap between the number of employees eligible to telework and those who actually do.

Telework participation has leveled out in recent years. As of 2018, 22 percent of all employees were teleworking and 51 percent considered eligible.

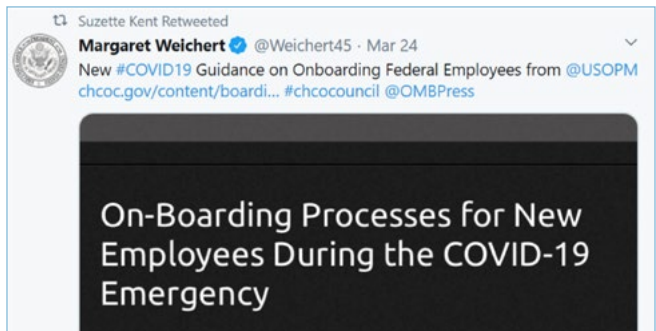


According to OPM's study, employees often choose to telework based on situational requirements, rather than a predetermined schedule.



Government IT Gets It Done

During the COVID-19 pandemic, social media has provided countless glimpses into the challenges facing government IT professionals. Here is a sampling.





Maintain productivity in times of crisis

Your government agency is on a mission to provide a seamless user experience, engage employees, and optimize resources for crisis management.

ServiceNow is committed to helping you manage the unique, rapidly evolving challenges presented by the coronavirus pandemic. Our digital workflows simplify complexity, so you can focus on what matters most.

Put technology to work during a crisis with workflow apps and resources to accelerate your response.

Learn more at [**www.servicenow.com/crisisresponse**](https://www.servicenow.com/crisisresponse)

Creating a Roadmap to Resilience

An interview with Bob Osborn, Chief Technology Officer, Global Government, ServiceNow

In the early days of the COVID-19 crisis, government agencies created a lot of make-shift processes and solutions to continue delivering services to the public, despite having many employees working from home. In recent days, they have shifted their attention to the future – not to returning to normal but preparing for the new normal.

The goal is to ensure resilience by creating an operational environment that won't be disrupted by whatever the next crisis might be. To learn more about building resilience, we spoke with Bob Osborn, Chief Technology Officer, Global Government, ServiceNow. He described a three-step roadmap to resilience, with each step supporting the others.

Response

The first step encompasses traditional activities in disaster recovery and business continuity (DR/BC): rapidly acquiring and deploying hardware and software, shifting the workforce from in-person to remote work, among other things.

COVID-19 proved more difficult for many agencies, Osborn said, because DR/BC plans typically assume that people and systems can be relocated to a new location, not scattered across a region.

To improve their ability to respond to a crisis, agencies need to improve the flexibility of the work processes underlying their operations and services. Whatever the crisis – and whatever resource constraints they are dealing with – agencies should be able to pivot quickly to adapt their processes to the new environment and roll out the changes to staff.

Readiness

Readiness is about being better positioned to respond to a crisis. It's about having accurate visibility into operations and services. For example,

understanding which technologies work together to support operations and deliver services, which parts of the organization use those systems, what dependencies are involved, and so on.

Once you have the visibility, “you can make the appropriate adjustments on the fly” when an event happens, Osborn said. In short, readiness improves your ability to respond. The two concerns go hand in glove, he said.

There's also a human element here, Osborn added: “You need to know who is empowered to make approvals on short notice to override traditional processes.”

Resiliency

Resiliency means having the ability to rapidly resume delivery of services after a disruptive event and to continue operating in that new environment as long as needed.

True resiliency goes beyond simply creating redundant capabilities that can ensure the availability of data and systems. It's about taking a holistic approach to the people, processes, and systems involved in delivering services and ensuring that all three aspects are addressed as part of a continuity strategy.

The ServiceNow platform is designed to help agencies create digital workflows that connect people, processes and systems. The platform is supported by a single data model and common application logic that makes it easy to automate processes and update those processes when requirements change.

“Our approach positions ServiceNow as a force-enabler for any agency responding to a crisis that they didn't see coming,” said Osborn.

Is This the New Normal?

It's hard to know what counts as normal anymore.

As the COVID-19 pandemic stretched on from March into April, into the summer and beyond, keeping many government employees at home, people began to talk about remote work as “the new normal.” That new normal included countless videoconferencing calls, disruptions from children also stuck at home and odd work hours.

That was expected to change once offices and daycare centers reopened, but as time went on, government leaders began to realize that some of the new ways of working were likely to stick, beginning with telework.

During the past decade, most government agencies have allowed a growing number of employees to telework at least occasionally. Agencies have scaled back in recent years, but as part of the COVID-19 response, many boosted their telework capacity and developed telework-friendly work processes.

At an April 13 briefing, DoD's Deasy said that the department has always had a strong telework capability, but that COVID-19 required it to bring in new capabilities – and that those capabilities were likely to stay.

“What we've now done is we've just put a multiplier effect into the quantity, the types of services, the collaboration tools, etc.,” Deasy said. “There will be some permanency to what we have here.... There is going to be an enhanced teleworking capability that will be sustained at the end of COVID-19.”

But the shift in thinking goes beyond telework. Many have developed new ways of doing business, with a focus on reengineering their workflows to work in a virtual environment. Agency leaders are now weighing which changes might be worth retaining.

Dorothy Aronson, CIO at the National Science Foundation (NSF), said officials must look at each change from several perspectives:

- What exactly does the change involve?
- Does it introduce any risks?
- Would keeping it entail changing any processes?
- Would it have an impact on any audits that are done?
- How does it fit into the agency's long-term vision?

Each change “is a little bit of a study of its own,” Aronson said. “You shouldn't just assume we're going to undo everything we did.” (See [p. 18](#) for a Q&A with Aronson.)

The public also might find that they like the new normal when it comes to digital services. Many agencies launched new services or expanded old ones to help deal with demand when offices closed.

“I think that we will see an acceleration of digital government because citizens have now been forced to engage government digitally,” said Delaware CIO James Collins. “They're going to get accustomed to getting services from anywhere, at any time, from any device. And I think that we're going to see an acceleration of investment.” (See [p. 30](#) for a Q&A with Collins.)



IT Gets the Spotlight

Whatever shape the “new normal” takes in the months ahead, IT will likely play a starring role.

The rush to remote work — to get employees set up to work at home and to adopt new solutions and processes to support that — has given government employees a new appreciation for CIOs and IT staff.

People who might think about the IT department only when things go wrong may now see IT as a critical partner in supporting the new government workspace.

“IT has never been more important,” said Theresa Szczurek, Colorado’s CIO and Executive Director of the Office of IT (OIT). “It really is our moment to shine.”

Szczurek said that her department plays two key roles. The first, of course, is keeping systems operational, especially during a crisis. The second is more motivational: driving innovation that can help the state be better prepared for the next crisis. (See our interview with Szczurek on p. XX.)

IT’s new high profile has the potential to translate into more influence.

That was the case at the General Services Administration (GSA), when it launched a progressive telework program about six years ago, CIO David Shive said.

“The CIO and the IT shop as a whole is seen as a trusted business partner to GSA because of this initiative and other initiatives like it,” Shive said. When GSA offices have tough business problems to solve, “IT is one of the first groups that they call to come around the table and think things through.”

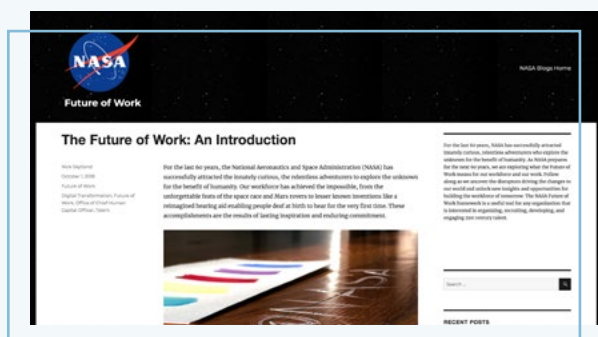
And IT professionals love to be part of an organization that recognizes their value, he said. “That kind of mindset at GSA makes it super easy for me to attract top talent into GSA...and I have some of the lowest turnover rates in the federal government.”

NASA Envisions a Modern Workspace

In 2018, NASA’s Office of the Chief Human Capital Officer launched its “[Future of Work](#)” initiative. NASA leaders wanted to understand how the workforce and workplace were evolving and the implications that might have for workforce strategies.

NASA found that technology was playing a critical role in that evolution.

“At the intersection of people, place, and technology is NASA’s need to enable its people anytime, anywhere. The traditional boundaries of our workspaces are disappearing because of advances in technology. Work, especially knowledge work, can now be conducted anywhere at any time by putting information, data, and tools at the fingertips of an increasingly mobile workforce. As the work and workforce evolve, the workplace must also adapt. Modern workspaces are being redesigned for greater flexibility and autonomy to enable teams to arrange themselves as needed to best work together, both collaboratively and individually.”





Security first.

It has never been more important to know that your collaboration solution is secure. For more than 15 years, Adobe Connect has been the solution of choice for federal, state & local government agencies operating virtual command centers for mission-critical operations.

Learn more at adobe.com/products/adobeconnect/rapid-response.html
To request a demo email adobeconnectsales@adobe.com



Adobe Connect

The Virtual Environment's Key Attributes

An interview with Alistair Lee, Senior Enablement Manager, and Peter Ryce, Product Evangelist, Adobe Connect

For many government employees, one of the biggest challenges of the remote work situation has been to continue effectively delivering on their mission critical operations.

Virtual environments have become mainstream and indispensable for a variety of use cases, whether it's large virtual gatherings, training sessions or meetings. It has been a paradigm shift, and if agencies can get it right, virtual environments could play a bigger role than ever even after the current crisis, reducing the need for travel, costs of large physical events, and providing more flexibility and reach.

But what makes a virtual meeting or training effective? To learn more about that, GovLoop spoke with Alistair Lee, Senior Enablement Manager for Adobe Connect, and Peter Ryce, Adobe Connect Product Evangelist. Adobe Connect is a web conferencing solution used for both meetings and training.

They highlighted three key attributes of a virtual environment.

Persistence

Ordinarily, virtual environments get setup and disappear along with the participants. Every time you hold a meeting, you need to start from scratch.

It is much easier to collaborate when the environment is persistent, that is, when you can set it up just once and use it over and over again. That includes not just the permanent URL, but also the access permissions, room customizations, shared files, content, chat and more — which is a real advantage for people who might have missed a session.

“Instead of thinking of it as a meeting you’re creating for a specific day and time, think of it as an always available digital room, preserving your content,” Lee said.

Engagement

Unfortunately, remote work can sometimes leave workers feeling disconnected from one another. Thoughtfully designed virtual environments can solve this with interactive features such as chat or polls. “That’s when we know they’re engaged, when we have their attention,” Lee said of workers. “It’s when they’re not being distracted by everything else on their computers.”

Dynamic virtual environments also make it easier for managers to track how engaged their teams are. These platforms contain engagement dashboards where leaders can see how invested their workers are in presentations. “As a host, if I watch my engagement meter start to decline, it means that I haven’t engaged my audience lately,” Ryce said.

Security

In many virtual environments, the default security setting is just a password. Once people get into the meeting, they have free rein. Adobe Connect takes a different approach by only giving control to the host, who can in turn grant rights to participants. “The guiding principle is least privilege — meeting participants should be able to access only those functions, like turning on their camera, that they specifically need,” said Ryce.

While going into a remote work environment was a learning experience for many people, it was familiar ground for Adobe Connect customers, who have used these virtual environments to meet during presidential elections, major sporting events, and to coordinate response during natural disasters.

Whatever the situation, remote work has demonstrated that a virtual environment is not just a fallback plan, but a valuable option for agencies even in normal working conditions.

At GSA, the New Normal Is Not So New



***An interview with David Shive
CIO, General Services Administration***

For many government agencies, the large-scale move to a remote work environment required a new way of thinking — along with new technologies and policies. That wasn't the case for GSA, which provides agencies with centralized procurement of products, services and facilities. For many years, GSA has been one of the federal government's leading advocates of telework, with a focus on providing employees with the tools they need to do their work securely at any time, from anywhere and using any device.

In April, amid the COVID-19 pandemic, GovLoop spoke with Shive about what the agency has learned about supporting a distributed workforce.

A Communicative Culture

In many ways, Shive said, the most important challenge in a remote work environment is also the most important challenge in a traditional office environment: fostering a communicative culture. GSA has done that, in part, by changing its physical offices.

What we've done is we've removed walls and cubicles and created open, collaborative workspaces. That doesn't just mean the practitioners doing the tough work of GSA — that's all the way up to the executive level. And that led to a collaborative culture in GSA where open communication in person, via email, via chat, via video, via all those mechanisms was just kind of the standard and the norm. So, when we switched over to the response to the national emergency, it wasn't a big change for how we operated.

From a technology perspective, the challenge was finding the right tools. But this was not only a procurement issue.

We had to make sure that those tools were vetted, that they were secure, that they met the business needs of the agency and that employees were trained on how to not just use the tools, but to maximize the tools' effectiveness. Again, the goal was to be able to do the hard work of GSA across all business domains from any location on any device both inside and outside the walls of GSA — and to make sure that the work was equally secure inside and outside. Let's use my own organization as an example. We have about 500 people on my team. Going into the national emergency, 18% of my staff were already full-time teleworkers, and over 90% did telework part time. So, when we actually flipped to full-time telework for everybody, it was kind of business as usual for us. We had some tweaking to do and stuff like that, but it was very lightweight, just to turn good outcomes into better outcomes.



Managing the Remote Workforce

Over the years, GSA managers have learned the importance of communicating regularly with employees, Shive said. When it comes to building trust, one key goal is to define expectations.

We encourage constant feedback and check-ins with employees. I always like to say we over-communicate. I don't think there's such a thing as over-communicating, but we communicate to a point where there is no doubt what the expectations of management are — and what employee expectations are as well, because that's a two-way street. This is not all about management laying an expectation on the employee. The employee rightfully has expectations of management as well. So, we build a two-way communication with them to make sure that happens.

It's also important to help employees understand how they fit into the organization's larger mission.

One of the things that keeps employees engaged is clearly laying out what our goals and responsibilities are as an organization and expressing to people what their part is in that. It's about being able to say, "Here are the organizational metrics, here are the metrics in your performance plan and here's where those two things tie together." And then when we celebrate meeting particular business metrics, we celebrate with the employees who made that happen. We're always focusing on the mission

statement and how we're driving toward meeting that mission statement. If they can draw that straight line between those things, it keeps them excited about being a public servant.

Hidden Measures of Success

Conversations about remote work often return to productivity: Are employees less productive when they are away from the office and dealing with the distractions of home? GSA has found that productivity typically increases, since employees don't have to commute, which takes time and energy. But productivity is not the only measure of success.

There's an organic kind of work that comes from people meeting in a hallway or around the water cooler, or sitting down and chatting while they're having lunch. That's where great ideation happens, where people say, "You know, we're doing this thing if it takes us four hours, but if we do it this way, we can get it done in three hours." We found that in a distributed workforce, a lot of that was lost. So, we were very intentional about reconstructing those capabilities in a virtual environment, so that you could have virtual team coffees and virtual lunch gatherings, where everybody would get together.

Such collaboration must become part of the normal workday, Shive said, because people work best when they have a good routine.

That's the key for any agency adapting to the new normal: making it the new routine.

Resilience During Unprecedented Change

Federal agencies are forced to do more with less to secure a remote workforce and maintain operational continuity. To meet these unprecedented networking challenges, Gigamon optimizes teams and tools to:

- + Ease the strain on overburdened VPNs
- + Secure a borderless network and increased attack surface
- + Reduce network disruption and inline tools outage
- + Maintain performance and good user experiences

When Networks Meet the New Tomorrow

The workplace continues to evolve. The unique demands of government agencies call for the right solutions to accelerate positive change and thrive in a new tomorrow.

Learn more about Gigamon solutions for government at gigamon.com/govloopCIO.

Gigamon®



Seeing Clearly With Network Visibility

An interview with Dennis Reilly, Vice President of Public Sector, Gigamon

Government IT networks are increasingly difficult to manage. Citizens want digital services that are equal to the private sector's. Cybersecurity risks, meanwhile, are multiplying daily. And the volume of data is growing faster than ever.

The COVID-19 pandemic complicated this situation further for federal agencies. Whether they're civilian or defense, these networks have been under unprecedented strain as most government employees have been working from home.

Network visibility can help agencies see all these challenges clearly and solve them. Using the right tools, agencies can continuously monitor their networks' performances and security.

Dennis Reilly is Vice President of Federal at Gigamon, a network visibility provider. Reilly shared with GovLoop three tips for better network visualization.

1. Identify the Logjams

As the number of remote workers grows, so does the potential for logjams on agencies' networks.

But agencies' networks don't have to buckle under their loads. Using visibility tools such as those Gigamon provides, agencies can see where traffic jams are happening on their networks in real-time. Subsequently, they can make quicker decisions that keep their networks flowing effortlessly. "It becomes a continuity of operations issue," Reilly said. "Agencies get the visibility they need to run at a high response rate."

2. Improve Customer Experience

Arguably, the most important interactions agencies have are with citizens. Consequently, the customer experience (CX) agencies provide must satisfy citizens, or they risk disappointing them.

Network visibility can help agencies by continuously monitoring how their applications and services are performing. Agencies with this awareness are better equipped to solve any CX issues that employees and citizens are encountering. **"Visibility is key to having applications run smoothly and stay secure," Reilly said. "If you can't spot a network performance bottleneck, you can't correct it."**

3. Stay Aware of Cybersecurity

As more agencies shift to remote work, cybercriminals and nation-state adversaries have also increased their efforts to attack them. As a result, endless vigilance is critical for defending agencies' networks.

Network visibility, then, meets two vital needs for agencies. First, it helps them detect and mitigate threats before, during and after attacks. Second, it helps them comply with all relevant cybersecurity regulations. The Continuous Diagnostics and Mitigation (CDM) program, for example, aims to reduce cybersecurity risks across the federal civilian government while increasing its overall IT visibility. By following DHS' guidelines and CDM best practices, agencies can gain stronger cyberdefenses.

Cybersecurity must remain top of mind for agencies because they handle citizens' sensitive data. Network visibility can assist agencies with protecting this information from any danger. "You want to see an attack as soon as possible to prevent a data compromise," Reilly said. "If you have been breached, you want to take action as soon as you can to prevent data exfiltration."

Ultimately, visibility ensures agencies don't blink on CX, cybersecurity and network performance.

What's Driving Your Modernization Strategy?



***An interview with Dorothy Aronson
CIO and Chief Data Officer, National Science Foundation***

Aronson's vision for empowering federal employees is far bigger than technology alone.

At NSF, she has been on a mission to create an environment where reskilling and upskilling are commonplace, and where employees are not only enabled to do their current jobs but also well-positioned to take on new roles in the future.

Work in Progress

For Aronson, the COVID-19 pandemic isn't driving her modernization strategy. Instead, it has expedited plans that were already in the works, including migrating on-premise data to the cloud, adopting the Zoom platform, and rolling out workflow software that supports e-signatures and automated document routing.

But what good are any of these tools if employees don't use them? In an interview with GovLoop, Aronson explained that NSF's ability to quickly pivot to fully remote work for employees and to conduct core operations virtually wasn't solely a result of having the right tools in place. These outcomes came from ongoing and collaborative dialogue between IT professionals and the end users who need the technology.

The priorities are to move continuous operations with continuous modernization. That's our mantra. And the reason for that is because IT is continuously changing [and] we have to continuously adopt and change with it. We have a very gradual approach to implementing these technologies, so we're always in the middle of deploying a few new things. And we do it at people's pace. We don't want to be disruptive to people's priorities.

She also credits the agency's nimbleness to the fact that nearly all employees have laptops that support their telecommunications and computing needs on a single device. But the pandemic has inspired people to more readily embrace technologies and new ways of working.

From our perspective, it was amazing how eager people were to learn and how easy it was. We had been through the evaluation and the procurement, we had already deployed to some early adopter customers and learned what the issues were.

Nearly overnight, the agency transitioned the core of its business — identifying and funding work at the frontiers of science and engineering — to a virtual environment. Although NSF had conducted some virtual review panels in the past to support inclusiveness, most were in person.

NSF's business is to receive ideas in the form of proposals, which are electronic proposals from potential researchers, and then we get a bunch of experts from around the country together to look at these proposals and assess them. Well...I should say around the world. And so what happens is, these panels often previously had been people coming to the National Science

Foundation. In addition to the activity of reviewing the proposal, the experts had an opportunity to get together and share their ideas. So the in-person panel has great value. But because of COVID-19, we went to 100% virtual.

Sizing Up Problems

Aronson said her approach to collaborating with end users doesn't involve bringing technology in as a solution, but rather asking people what their problems are and determining whether technology is a part of the solution. The biggest mistake IT people make is starting with IT, she said. NSF has reversed that model through the use of democratized IT governance groups, where technology professionals are embedded with people who work in key program areas.

When asked what she's learned from responding to COVID-19 and supporting the workforce, Aronson highlighted what she's learned about herself and others.

There were opportunities that I wish we could have taken that we didn't take. That's where I feel it. But it's not the same as a mistake. I really think that it's important for us to understand that, under pressure, people behave differently and are surprised by those differences. And that we really, as leaders and managers, have to be very, very human and tuned into those emotional situations because they creep up on everyone, including us.

That's why Aronson is creating opportunities that provide a sense of belonging for her team, especially those who weren't immediately supporting COVID-19 response activities and needed a sense of purpose. At least one employee has taken her up on the offer to get training and build her skills. She's learning R, a programming language used for statistical computations and data analysis.

I'm trying to get the people who are floating away a little bit to adopt some of these future technologies. Just one person at a time, right? That's how I'm working on it right now.

So, I'm trying to build a community of people that are doing that kind of thing. I'm thinking of it as a book club. If we all take the same course at the same time, we can talk about it, like you've read the book. So, that's one of the things I'm worried about right now: how to get the book club together.

Not Just Talk

Aronson's parting words of wisdom for her colleagues in government are to push through and keep on course with modernizations efforts. They are more critical now than ever. The vision for the paperless office and entirely mobile workforces isn't just talk. It's a requirement.

It's the continuous modernization and the continuous move forward that allows this to succeed.... People need to be on technologies that are flexible, that can continue to move forward. I hope that people will find replacement of legacy stuff and that the standard should be to be at market level with your IT and always moving a step ahead.





Red Hat

Digital transformation the open source way

Open technology. Open culture. Open process.

Drive transformation with redhat.com/gov

The 5 Elements of Government Digital Transformation

An interview with Dmitry Didovicher, Digital Transformations Architect (DoD/IC), Red Hat

How do you define digital transformation? Many people talk about the technology that enables transformation – and how that technology is acquired, deployed and managed. But at a higher level, you might also say it's about culture – about how an organization approaches the work of developing and delivering services.

This is what Red Hat calls Open Transformation. To learn more, GovLoop spoke with Dmitry Didovicher, Digital Transformations Architect (DoD/IC) at Red Hat, a provider of enterprise open source software solutions. He discussed what Red Hat calls the Five Elements of Transformation.

Leadership

In the context of digital transformation, leaders who embrace an Open Organization culture create a shared vision for the work to be done and to define the measures of success and failure, Didovicher said.

Leaders often focus only on defining success, “but it’s not a rapid success story that drives innovation, it’s a constructive failure,” he said. That’s because when something succeeds, things tend not to change. When something fails, on the other hand, it leads to fruitful conversations about what needs to change and how.

Product Management

Didovicher’s advice? Forget the term project management. That’s tied to old-school, “waterfall” methodology, which takes a drawn out, linear approach to the development lifecycle.

Instead, he said, Open Organizations need to focus on Product Management through Product Ownership. A product owner is not focused on an end goal but on the continuous delivery of new capabilities to strengthen the product. That is how transformation happens.

Development

Just as project management needs to shift to product ownership, development needs to shift to modern Product Deployment. Clearly, the transition to cloud-native

software – leveraging containers and Kubernetes – puts an emphasis on speed and agility. But that doesn’t mean giving developers free rein, Didovicher said.

Organizations need to give developers the functionality they need, but that functionality needs to align with the enterprise digital architecture. Providing that framework “gives them freedom but guides them toward deliverables that are of value to the enterprise,” he said.

Architecture

Any mature development organization will have a Vision Architecture to guide its product development work. But when it comes to transformation, they need what Didovicher calls an enterprise digital architecture.

The goal is to define an enterprise-level strategy for product delivery, addressing everything from the Trusted Software Supply Chain and compliance processes to API management and OpenShift powered Software Factory for your containers and micro-services. Vision Architecture shows how these tools tie together to support the Open Transformation, Didovicher said.

Operations

Advanced operations through competencies such as Site Reliability Engineering (SRE) is about looking at transformation from an operational perspective. How well does a new digital service meet enterprise requirements for performance, reliability and security? Didovicher recommends that organizations should establish an enterprise-level minimum viable product (MVP) that lays out key requirements that all products must meet.

In advising agencies going through an open transformation, Red Hat is not pushing a solution. Instead, these five elements are designed to help agencies think about the key decision areas they must address.

“They’re not mapped to a technology at all,” he said. **“The five elements map to success stories that have been proven time and time again – including at Red Hat.”**

How Crisis Can Drive Innovation



An interview with Theresa Szczurek
CIO and Executive Director of OIT, Colorado

For Colorado, the COVID-19 pandemic could be a turning point. In adapting to the crisis, the state's Office of Information Technology (OIT) has found itself in a position where it can accelerate its push for IT transformation because the crisis has already put transformation at the top of the agenda.

It's a new environment in state government, but not so much for Szczurek. When she worked in the private sector, she ran several entrepreneurial high-tech ventures, including one that was completely virtual. GovLoop spoke with Szczurek about how OIT responded to the crisis and how it's shaping its future.

Operations and Innovations

Szczurek said that the IT team's work has never been more important than it is now. OIT has proven instrumental in helping the state government respond to rapidly evolving requirements.

I break our work into two big buckets. One is keeping systems operational, especially in the time of COVID. The other has to do with innovation — the work that we can do to help the state and our Coloradans handle this better. Overall, I like to think of myself in a “motivation and direction” role with regards to all of that. The state has been looking to the Governor's Office of Information Technology as the enterprise provider of technology support and services to really help move employees into a telework situation, to keep all of our state applications operational and be able to address any challenges going forward.

During the pandemic, 90% of OIT employees and 75% of all state employees were working from home. In some ways, the task of creating this remote work environment was clear-cut: buy more equipment, get people situated and increase network capacity. But innovation was often a necessity, such as to support the help desk, for example.

We found that our service desk started getting a huge increase in load. So, in the innovation area, one of the things we did was start more quickly diffusing a tool for password self-service resets, since that was the largest need that people were calling in to the service desk. Now, we have all but a couple of agencies equipped, which has greatly decreased our service desk demand. We got more people in the service desk so that we can deal with that demand as much as possible. But another thing we've done is hold “office hours” on a regular daily basis, so that people could call in at a certain time.



The state also has leveraged virtual solutions to meet emerging needs. This approach is giving OIT an opportunity to consider the role that such solutions might play in the long term.

We are always looking to improve efficiency, transparency and customer satisfaction. And, you know, one of the things in this time of crisis is you have to act fast.... [For example], when we saw that the Public Health and Environment [Department] and other agencies were having a huge increase in the number of calls coming in, we stood up some virtual call centers based on a pay-as-you-go model, and this really allowed us to meet that need quickly. And we've had to move toward electronic document signature and other new products. Now, as we are looking back, we're learning lessons and we're seeing what we want to keep and what we don't want to keep.

Social Change Theory

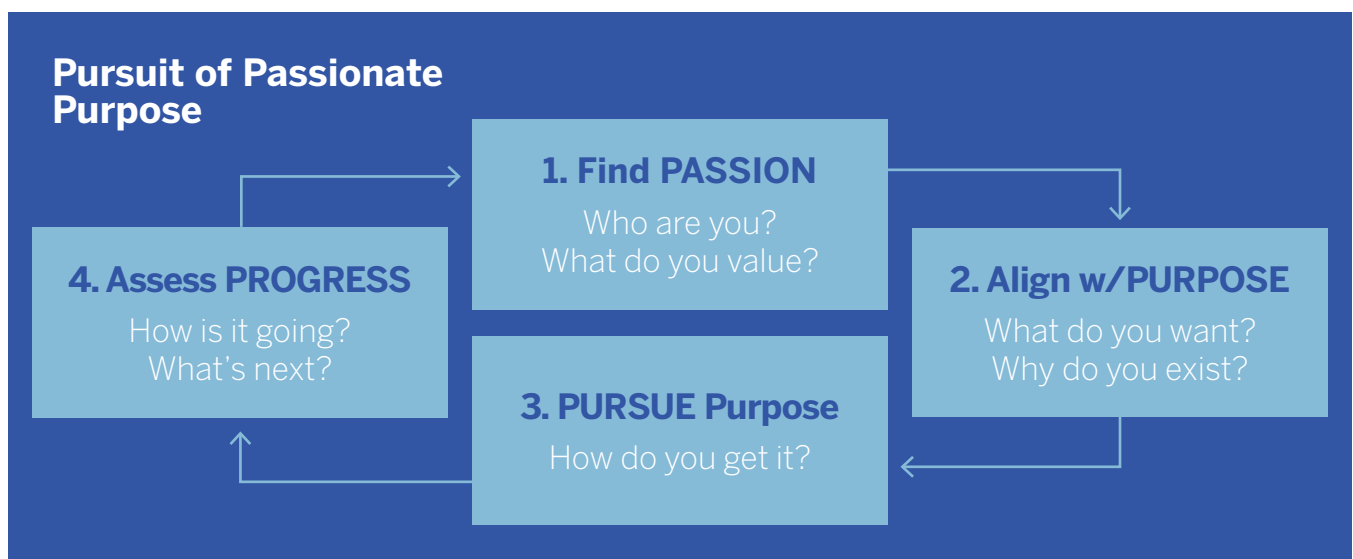
OIT had launched an IT transformation initiative before COVID-19. Szczurek believes that after the crisis, that initiative could gain more traction.

I like to use this model by Kurt Lewin called social change theory. Lewin talks about being frozen in a certain situation with a set of forces both positive and negative — forces that hold people or a situation in place. If you want change, you need to unfreeze the situation — like melting ice cubes — so that you can align with the positive

forces that encourage change and get rid of some of those negative forces that resist it. The COVID-19 situation is an opportunity because we are unfrozen. You don't want to waste a good crisis, so to speak. We can see where we were at before, get aligned with the governor's vision of IT transformation, and then work through processes and products around talent, governance, technology, security and service — how can we better serve the state? — and then refreeze it.

Szczurek recognizes that such tumultuous times can be challenging for employees. She believes that the key is to help employees tap into what she calls “passionate purpose.”

I did a major research study on this prior to coming to the CIO position, and I asked people what brings meaning to your life, what helps you continue working towards a goal. And people said two things: It was the opportunity to contribute and the opportunity to make connections. So, I asked, “How do you do that?” And it's by lighting a fire. This is where people need to connect with their passion and align that passion with a meaningful purpose — I call it a passionate purpose — then pursue that purpose with a plan, assess progress...and then reset for the next wave. This is a four-stage model that I like to depict in a circle. I call it the Sacred Circle of Life, because we do this in our personal life and our professional life.





BlackBerry Spark

Unified Endpoint Security:
Bridging the Gap Between

Zero Trust & Zero Touch



Learn More at: <https://www.blackberry.com/us/en/solutions/unified-endpoint-security-ues>

899.23

Unified Endpoint Security: Bringing Order to Chaos

An interview with John McClurg, Senior Vice President and Chief Information Security Officer, BlackBerry

In cybersecurity, organizations create chaos with the best of intentions. Their goal is to make incremental gains in security by implementing new solutions that make up for the deficits of older ones and adding new controls to compensate for the limits of existing ones. To make matters worse, the IT environment itself has grown more complex, creating new attack vectors that malicious actors can exploit.

Clearly, agencies need to reduce the chaos and improve security. But they also need to ensure their cyber strategy does not hinder employee productivity. Those competing needs were more apparent than ever when gubernatorial mandates in response to the COVID-19 crisis required thousands of employees to begin working from home, some using their own devices. How could agencies protect applications and data without creating new obstacles for employees?

To learn more about how agencies can take a more cohesive approach to endpoint security, GovLoop spoke with John McClurg, Senior Vice President and Chief Information Security Officer at BlackBerry, a provider of intelligent security software and services.

“Quite often, if we pursue security in the way we want to, we end up leaving our users with just a horrible experience, because of the ‘friction’ they incur,” McClurg said.

A Modern Solution

The solution to these challenges is not another product. That would only add to the chaos. Instead, McClurg said, agencies need to shift to the emerging concept of unified endpoint security (UES).

Unified endpoint security leverages artificial intelligence, machine learning and automation to provide next-generation cyber threat prevention and remediation across devices, networks, apps and people – all without interfering with user productivity.

“It’s a modern solution for a challenge that we have faced for decades,” McClurg said. Specifically, it is designed to shift agencies to thinking in terms of preventing cyberattacks, not just reacting to them, he said.

From a security perspective, UES implements the concept of Zero Trust security. Zero Trust is a dynamic approach that continues to evolve as it learns from user behaviors and as your environment changes with new users, new devices, new applications and new technologies. One of the concerns about Zero Trust, however, is that it will create countless obstacles for employees who are just trying to do their jobs.

That’s why the concept of Zero Touch is essential to UES. AI, machine learning and automation allow for authentication as a continuous process. The idea is to leverage operational network data to create and refine behavioral profiles of users and devices, so that the network can identify them without any human intervention. That’s why it’s called Zero Touch.

“There doesn’t have to be that dichotomy and that tension between providing security and positive user experience,” McClurg said. “The dichotomy dissolves as you leverage the benefits of what the endpoint security solution set now affords you.”

BlackBerry has identified six pillars of UES:

- Endpoint Protection
- Endpoint Detection and Response
- Mobile Threat Defense
- Continuous Authentication
- Data Loss Prevention
- Secure Web Gateway

Creating UES would be just another challenge for agencies if they had to start from scratch. BlackBerry has developed solutions with UES in mind, ensuring integration across those pillars. Current solutions address the first four of the pillars, with the other two in the works.

'In Every Crisis, There's Opportunity'



An interview with Sylvia Burns
CIO, Federal Deposit Insurance Corporation

It's difficult to change how people work, but inevitably, the pandemic has forced government employees to change their habits.

The opportunities for technology to be adopted and embraced like never before is the silver lining that Sylvia Burns, CIO at the Federal Deposit Insurance Corporation (FDIC), sees at both her agency and the federal government at large during this crisis.

"I have seen in my experience that in every crisis, there's opportunity," Burns said. "In some ways, it was the biggest help we could have gotten in terms of organizational change management and getting people to embrace technology."

GovLoop interviewed Burns to find out what changes the federal agency underwent and what opportunities the crisis unveiled.

Digital Signatures

One of the first ways work needed to change was document signing. The agency already had tools for e-signing, but most employees did not use them because they were accustomed to wet signatures, or signing on paper. Federal policies aside, people had neither reason nor desire to change the way they were working.

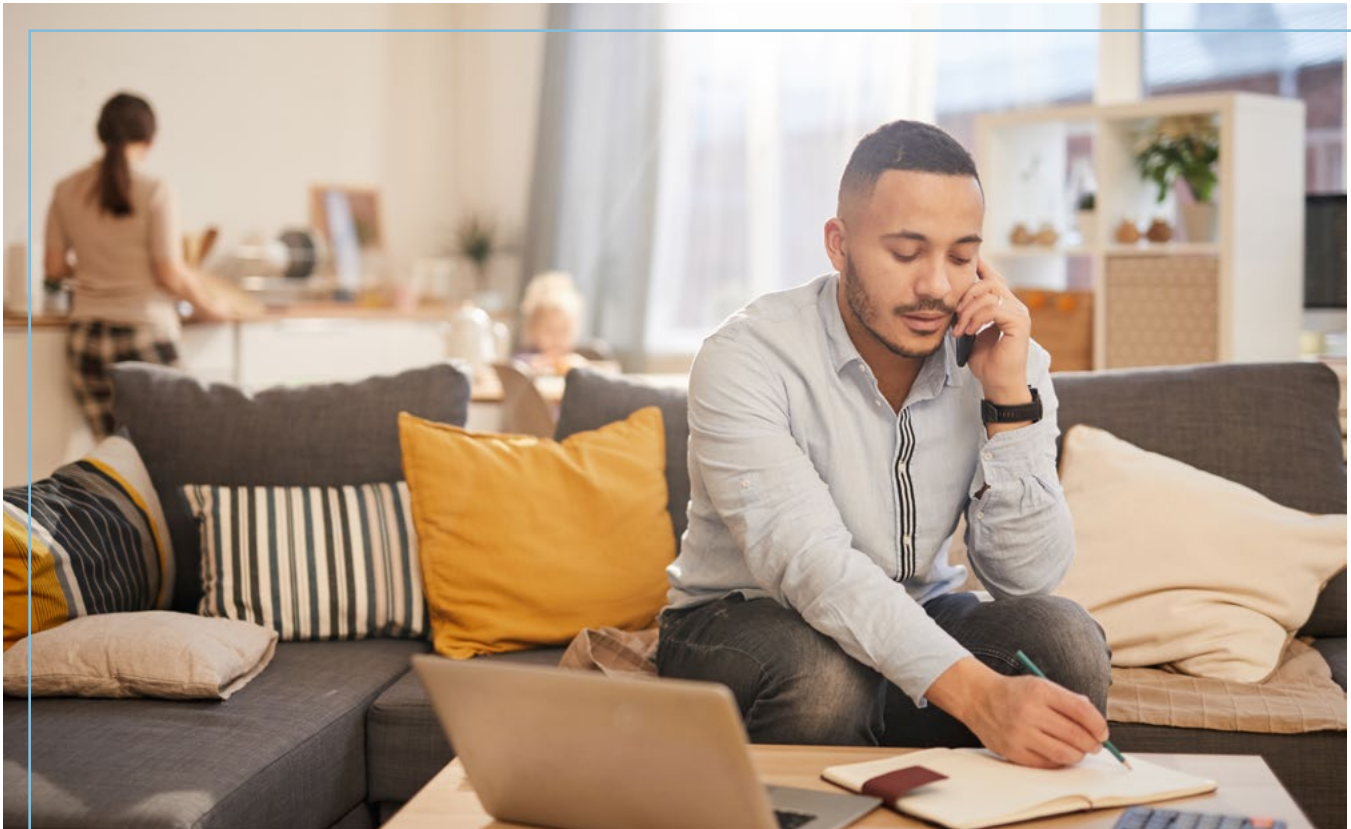
I know at the federal government level, [the Office of Management and Budget] is trying to strongly push digital signatures. They've had policies about [these] things in the past. When you throw it out there in a non-crisis environment, it's hard for people to embrace that.

When FDIC's workforce shifted to telework in March, e-signature tools were no longer an option, however. They were the only way to sign papers. As a result, the scale at which these tools were being used

increased dramatically, and various offices within the agency came to the IT division for help.

We ended up going and working with our legal division to help us understand the legal aspect of signing documents. And they dispelled some myths.... Some people thought they had to sign documents that they didn't have to sign. And it was because over the years, somebody at some point said, "Let's sign this document when we transmit it." Well, we found there were no legal or policy requirements that some of these documents needed to be signed. If you transmit the document through an official FDIC system like email, they're considered official.

By embracing e-signature technology, the agency found and eliminated an extraneous procedure in the process and improved operations for the future.



IT and Business Are Closer Than Ever

During the crisis, the relationship between IT and business has grown closer, Burns said. “The business needs IT to keep productive, and vice versa. We need the business,” she said.

For example, the agency is responsible for ensuring that depositors of FDIC-insured banks do not lose their deposits if that bank fails. The process for responding to a bank failure is called Resolutions and Receiverships.

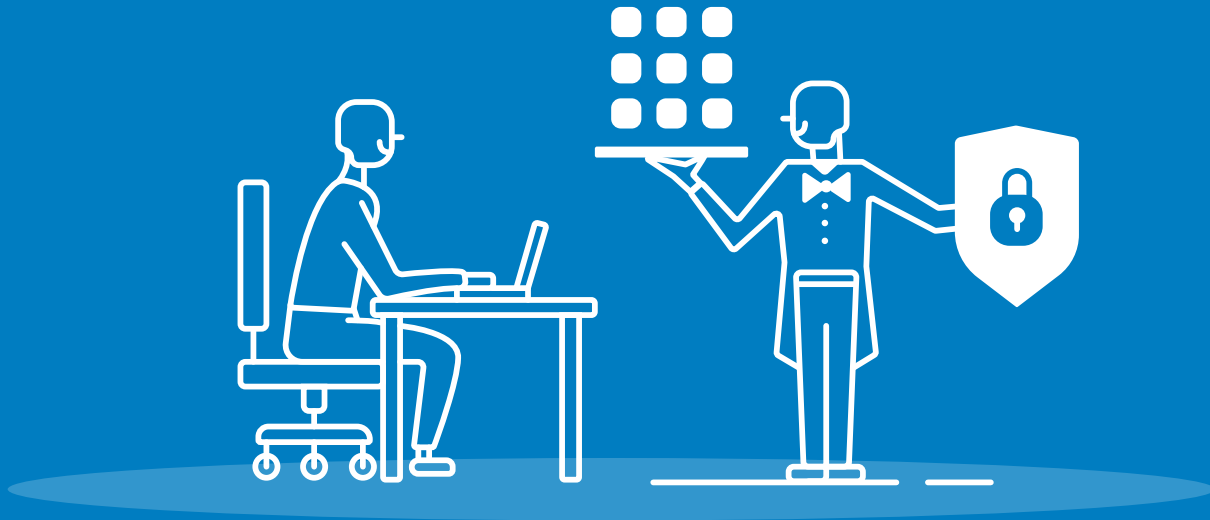
The traditional process for that involves sending dozens of people onsite to that bank to actually do the closing. In the world we’re in right now, with the pandemic, we want to minimize the amount of people that we send anywhere. So what does that mean again? It means you have to look at technology.

Burns is actively researching remote and automated tools for essential business operations that will minimize staff’s physical exposure as much as possible.

There’s little likelihood that after turning to technology, they will return to manual methods.

I think this whole situation is creating a new normal. I’ve talked to a number of people over the last few days about not going back to the manual, old way that we used to do things because all of a sudden, we’ve proved through this crisis that we could do things differently. We could minimize the number of people needed to go to a bank closing. Maybe 50 people could be on the back end using all the tools and technologies to do the processing work, and maybe you only send 10 people, instead of 60 or 70.

Basically, this situation has been almost like a live proof of concept, and in many cases, things have been proven. I would say that some of my colleagues who lead other mission areas of the FDIC are saying, “Well, you know what, why would we go back?”



Helping to protect your agency's remote workforce by ensuring government employees, contractors and partners, have simple and secure access to mission critical applications from any device at any time with the Okta Identity Cloud.

- Single sign on for on-prem and cloud apps
- Granular access policies based on user, device, network and location context
- Strong multi-factor authentication across all apps and VPNS

Learn More: [Securely Enable Remote Work](#)

Identity Access Management in the Telework Era

An interview with Kelsey Nelson, Senior Product Marketing Manager, Okta

Nationwide, agencies have embraced telework during the COVID-19 pandemic. While most agencies have rapidly transitioned to remote work, it hasn't been without challenges. Many agencies couldn't provide remote access to systems except email when the crisis first hit and as a result, workers couldn't access many of the systems they use daily.

At the same time, threat actors haven't been sitting still, and attacks such as phishing and spear phishing are on the rise. Now, traditional network-oriented security isn't sufficient with users accessing resources from more locations and devices than before.

That is why identity and access management (IAM) is critical to helping agencies navigate this new normal. IAM covers the policies and tools ensuring the correct people have the appropriate access to organizational resources.

Kelsey Nelson is Senior Product Marketing Manager at Okta, a cloud-based IAM provider. Nelson shared three ways IAM can improve agencies' teleworking cybersecurity.

1. Practice zero trust

Zero trust cybersecurity involves never assuming trust for any entity inside or outside an agency's IT perimeter. It is a modern security strategy that helps agencies manage, monitor and secure their data across all their applications, devices, networks and users.

According to Nelson, the COVID-19 outbreak has pushed the need for a zero trust approach to security to the forefront of IT and security leaders' agendas. **"Zero trust isn't something that we're building toward or that we want to enable conceptually in the future," she said. "It is today. Everyone is outside the perimeter."**

As agencies begin down this zero trust path, starting with a strong foundation in identity and access management will not only help strengthen security for agency workers, contractors and partners, but also help make it easier for them to get to the tools they need to be productive.

2. Understand users

Agencies need to find ways to continue to drive productivity without compromising security. At the end of the day, users will find ways to circumvent security controls if they become too cumbersome to do their work. Granular access policies based on their devices, networks, users and location context can help keep agencies improve both security and the end-user experience.

These policies give employees only the access and tools needed for their jobs and also weigh risk of each authentication. If the risk is low, agencies can choose a more streamlined access experience and if the risk is high, agencies can set policies to require multi-factor authentication via the factor of their choosing. This policy framework makes it simple for both IT and security leads and end users.

3. Find ways to automate

Onboarding and offboarding workers, contractors and partners is always a challenge for agencies, but even more so when workers aren't able to come to the office.

Using identity solutions to automate provisioning and deprovisioning will be a critical way to both help IT teams streamline manual, often error-prone tasks like this and also for agency workers to start work as efficiently as possible. And, in doing so, it'll help agencies mitigate the risk caused by latent access, orphan accounts or incorrect access provisioning.

Whether it is on-premises or remote, IAM can help shield agencies from any cyberthreat – and get workers back to helping achieve their mission as quickly as possible.

Delaware's Path to Digital Service Delivery



***An interview with James Collins
CIO, Delaware***

In late April, more than 30 million Americans filed for unemployment benefits as the economic fallout of COVID-19 closed workplaces and devastated businesses.

Their rush to already overwhelmed government unemployment services sent claims and inquiries soaring, and government IT systems nationwide floundered because of the surge. Websites crashed and claims stalled, delaying unemployment benefits disbursement.

But the Delaware Labor Department website didn't crash, not even once. In fact, it added new features. The reason for the state's success was the relationship building, information sharing and preparation of technologists, James Collins, Delaware's CIO, said in a late April interview with GovLoop.

Understanding Pain Points

You've heard all across the nation about unemployment issues and how the departments of labor nationally are struggling to keep up with the demands of unemployment benefits, which are critical for people being able to pay their bills, take care of their family. So, we got engaged in a conversation with [our Labor Department], and they were struggling with some things that we could be helpful with. We weren't the first thought of, "Hey, let's talk to the CIO or the IT people about this." They were just doing the best with what they had available to them.

In the Department of Labor, they have an Unemployment Insurance Division. That's where their demand has increased exponentially. They're processing in a week what they processed in months before. And so, behind the scenes, we added some processing power, some horsepower — however you want to put it — to their infrastructure.

Collins' team didn't just package up added servers, CPUs or RAM. Although IT did increase processing power, which ultimately prevented the website from going down, Delaware's Technology and Information Department (DTI) went beyond technobabble.

After making sure everything worked, the team added common-sense functionality for employees and the public.



For example, for employees, Collins and his team added a monitoring function to Labor's online resources. That way, if the department saw a rise in visitors and users, it could contact IT to preemptively add more processing power. For the public, DTI added automated tracking messages, like the ones online shoppers receive, to unemployment claims. By sending these tracking messages, Labor can reduce the number of inquiries and lighten stress on call centers and websites.

Those are nice messages, but they have a purpose. They don't want me calling asking about my package. They don't want me having any insecurity that my order's been received, that it's being processed, that my package is being shipped. That's how they get all these calls coming asking questions. And so, we just laid out some of those strategies to the Department of Labor. That resonated with them immediately.

We're in the process of being able to roll out some of those proactive communications that are going to be a win-win. It's going to be a win for Labor because they're not going to be deluged with inquiries. It's going to be a win for those people who need to access those resources to know that [their] benefits are being processed.

Building on Groundwork

Delaware's IT team was well equipped to deal with COVID-19, in part because of regular communication with other states; the National Association of State CIOs (NASCIO), which Collins was president of; and other Delaware departments, he said.

Collins emphasized that he was just one call away from Delaware's service-providing departments — a connection he established long before the pandemic. Regularly, he'd pop into offices to build an understanding of their needs and wants. The role of his staff is to support those departments' missions, Collins said.

It's a result of a lot of groundwork on behalf of not only our IT team, but the CIOs' IT teams across the nation. We can't really have a conversation about innovation if you're not nailing the basics. If you think about it like this, you don't really think about your electricity provider often, because it just works. And until there's some type of crisis, and you're like: "Oh, it's not working. What the heck?" That becomes a crisis in and of itself.

Recently, some state employees sent Collins emails thanking him and his team for enabling the virtual delivery of critical government services,

from education to press conferences to health care. He's always quick to share that feedback in town halls with his staff, which is entirely remote.

But Collins also noted that technology has had these abilities for a long time. Digital government, he said, is flexing its muscles right now and showing why it and the people behind it deserve their time in the spotlight.

I also think that we will see an acceleration of digital government because citizens have now been forced to engage government digitally. They're going to get accustomed to getting services from anywhere, at any time, from any device. And I think that we're going to see an acceleration of investment.





You have goals. We can help you get there.

Reduce risk across your entire connected environment. Rapid7 gives you full visibility, analytics, and automation to help you more easily manage vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate your operations.

LEARN MORE: Visit us at www.rapid7.com

RAPID7

Election Security Is About More Than Voting Machines

An interview with Tod Beardsley, Research Director, Rapid7

Conversations around election cybersecurity have gone mainstream. Much of those discussions focus largely on voting machines and known security flaws that hackers can use to compromise the technology. But that's only a fraction of the larger issue.

"To ensure the security and integrity of our elections, the focus must be on the IT infrastructure that supports and runs our democracy, rather than exclusively on voting machines themselves," said Tod Beardsley, Research Director at Rapid7. It's an issue that's top of mind for Rapid7, which offers a suite of solutions, including 24/7 threat detection and incident response and penetration testing. The focus is to help teams secure their environments and build out their programs in alignment with industry standards.

Today, as a pandemic rages across the globe, government agencies are exploring alternatives to in-person voting to promote social distancing. Even still, cybersecurity must remain an integral part of the conversation.

Beardsley outlined key issues around election security that should be top of mind for agencies.

1. Lack of planning and execution today for whatever comes.

Election Day isn't far off, and there's still a fair amount of coordinating and planning that must take place. "We have over 8,000 voting districts in the U.S., and I am not confident that we are doing enough to secure the election, both in a cyber and a public health way, to meet this deadline," Beardsley said.

What's at stake is the same old second-order problems we've seen. Voter information websites and databases continue to operate on rickety, poorly-maintained software, especially in low-population districts, he said.

2. Experimental internet voting platforms.

Beardsley believes that internet voting will be possible, but 2020 is not the time to roll it out. The reason? The applications on the market today are grossly insecure and have some severe availability problems in production.

"Absentee balloting seems to be the best possible option, but this turns out to be, bizarrely, partisan," he said. "To be clear: Vote by mail does ruin the tradition of a secret ballot for many people, but the trade-off seems to be worth it to ensure reasonable levels of participation."

3. Low turnout means a greater return for attackers.

Attackers who seek to disrupt the vote will fare better when fewer legitimate voters show up.

"High turnout would tend to suppress the actions of a few attackers, no matter how successful the attacks are," Beardsley said.

His team works with agencies to secure their environments by proactively monitoring their networks and devices or by implementing technologies and processes. The goal is to help agencies quickly respond when a breach occurs and assist them in a variety of ways.

Ultimately, agencies must be on guard and prepared to ensure the integrity of our nation's elections.

The Nuclear Regulatory Commission's Remote Work Success Story



*An interview with Dave Nelson,
CIO, Nuclear Regulatory Commission*

Of all the federal agencies, the Nuclear Regulatory Commission (NRC) needs more reliable remote work than most. NRC protects the public's health and safety by regulating civilian nuclear energy.

Nuclear materials can endanger everything from the public to the environment, so the agency can't afford serious disruptions to its work. But that's just what COVID-19 brought: serious disruption.

In NRC's case, gone are the days when its headquarters hosted most of its workforce. Instead, COVID-19 forced scores of employees to work from various locations. The resulting arrangement was unlike any the agency had experienced.

Fortunately, the agency shifted gears with few glitches. Its transition to remote work now serves as a case study for other agencies to follow during future crises. More importantly, COVID-19 has taught NRC valuable lessons about agility, leadership and effectiveness.

GovLoop spoke with CIO Dave Nelson about insights the agency has gained into remote work. The coronavirus outbreak has made the agency's workforce, technology and tactics stronger, Nelson said.

COVID-19 Chaos Hits NRC

In March, agency leaders decided COVID-19 directly threatened the workforce. Subsequently, NRC adopted mandatory telework for most of its employees.

But functioning remotely proved easier said than done. NRC quickly encountered two hurdles to teleworking: people and technology, Nelson said. People were scared that the network wasn't going to hold, based on previous experiences with snow days and power outages. And this time they had

to plan to be out for weeks. Nelson said NRC also discovered many of its employees were reluctant to use unfamiliar tools for working remotely.

There's an element of change management required there. We had all the technology in place, but people weren't leveraging it. There's a reluctance to change even if you have that ability. There's this concern that it's a hassle to learn new things.

Together, NRC's human and technological issues could have slowed its COVID-19 response. NRC overcame both obstacles by focusing on its employees first. By teaching workers how to view their tactics and tools differently, most of NRC ultimately embraced teleworking.

If there were any doubts, they're gone. We've proven we can maintain our business and our mission working from home.

Tackling Telework With People

How did the agency quickly leap from its usual routines to teleworking amid a global pandemic? The agency identified and fixed the skills employees were missing to effectively work remotely, Nelson said.

We knew we were all going to work from home. Many of the members of our staff didn't have direct experience with remote working or the technology. We needed to make sure we were ready, and our people had all the right things.

As a result, NRC began rapidly teaching its staff how to use its remote work capabilities. Using the agency's exhibition center, Nelson's team began instructing interested employees about the tools available to them.

One week before NRC started teleworking, participants heard about options including Skype and virtual-private networks (VPNs). VPNs let users send or receive data across shared or public networks without directly connecting their computing devices.

People see the technology working and they get confidence. People know they're being heard. Those kinds of things keep the trust in place.

NRC didn't stop evolving after launching its telework efforts, however. Nelson said NRC began tracking workers' opinions with real-time online polling.

It's reaching out to them and making sure they're OK. We're asking about the coping strategies people have.

Upgrading NRC's Networks

Training wouldn't help NRC's employees telework unless they also had the tools to succeed. NRC closely investigated its networks to make sure they were ready for remote work, Nelson said.

We tried to stress our systems and our people and see what problems they had. Our network architecture people had a good theoretical sense of what our networks can support. But we learned a lot.

NRC's tests revealed that its networks lacked the bandwidth to enable agencywide teleworking. Nelson said they addressed this by requesting an urgent bandwidth increase from its service provider.

I've never seen the major carriers move as fast as they were during that time. Within days, they were installing major new services for agencies.

Although beneficial, NRC's network upgrades left it with more to defend from cyberthreats. Nelson said NRC made sure it fortified its entire attack surface before embracing telework. Agency data often covers nuclear reactors, materials and waste, so the agency treats it cautiously.

Now, NRC's concern for how teleworking impacts its technology and workers is helping it weather COVID-19. According to Nelson, the agency is doing its part to help the federal government operate smoothly during this difficult time.



Remote everything. We've got you covered.

Powerful, easy-to-use remote monitoring software and tools
from solarwinds.com/solutions/secure-remote-access



ACCESS RIGHTS
MANAGEMENT



ACCOUNT
TAKEOVER
PREVENTION



SECURITY
INFORMATION &
EVENT MANAGEMENT



PATCH
MANAGEMENT



CONFIGURATION
MANAGEMENT



MANAGED FILE
TRANSFER



REMOTE
CONTROL

How to Meet the IT Management Challenges of Remote Work

An interview with Brandon Shopp, Vice President of Product Strategy, SolarWinds

Throughout the COVID-19 crisis, government agencies have learned two basic lessons about remote work. First, the experience has diminished doubts about whether employees could work effectively and efficiently outside the office. Second, it's made IT leaders aware they need a better strategy for managing this remote environment.

To learn more about how agencies can ensure the security and performance of the remote work environment, GovLoop spoke with Brandon Shopp, Vice President of Product Strategy at SolarWinds, which provides IT management and monitoring solutions. Shopp highlighted three key security and monitoring capabilities.

Threat Monitoring

One reason the remote work environment has been so challenging from a security perspective is because it introduced a whole new range of threats. Employees are using their own internet service providers, and they're sharing a network with family members or roommates whose devices likely aren't secure. It's a whole new attack surface area.

It's critical to know what threats are present in this environment. During the crisis, for example, there was a surge in phishing attempts with a COVID-19 angle (e.g., "Click here for an update on COVID-19 in your area"), opening the door to a ransomware attack. Agencies have a better chance to block these threats if they know they're coming. This is the value of a threat monitoring service.

Security Event Management (SEM)

SEM provides agencies with deep insight into activity across the network. Using network logs and other operational data, SEM identifies patterns of user and system behavior. This makes it possible to recognize anomalies indicating possible security threats, such as unusual file changes or shares.

SEM is particularly important in a remote work environment because it helps IT teams understand new patterns of behavior. "In this time with everyone working at home, you're going to see new anomalies in terms of behaviors, and so you want a solution that can centralize and aggregate all that data and help you make sense of it," Shopp said.

Network Configuration Management (NCM)

NCM is another capability taking on new importance in a remote work environment. NCM provides visibility into the state of your network infrastructure, monitoring how routers, switches, load balancers and other network devices are configured and managing any necessary changes in configuration. This insight makes it easier to manage the network as requirements change.

Remote work, of course, brings significant changes, especially with so many employees connecting to the network through virtual private networks (VPNs). Most agency networks were not designed to handle this much VPN traffic, requiring them to make quick changes and often resulting in configuration errors leading to down time. NCM makes it easier to visualize and troubleshoot problems and make the necessary changes.

More than anything, the experience of remote work has taught IT managers to think in new ways about the enterprise, Shopp said.

"Agencies can't assume anymore that employees are going to be within the four walls of an office," he said. "They've got to think broader than that. They've got to make sure they have the right infrastructure so that their employees can do their jobs and support the mission of the agency."

Best Practices

Strategies for dealing with the next crisis

Managing Teleworkers: The Basics

GSA offers the following suggestions for managing teleworkers:

- **Facilitate a teleworking protocol meeting with your team:** Host a conversation to identify your team norms and protocols to reach a consensus on what “teleworking as a team” means for you.
- **Build a trusting environment:** Use telework as an opportunity to foster trust between employees and managers. Established and agreed upon metrics for productivity help ensure teleworking success and reduce the need for rigid monitoring or micromanagement.
- **Monitor performance:** Hold employees accountable for their work fairly and promptly. Telework does not create inefficiencies, but potentially exposes them. Offer multiple check-in opportunities for your team together and individually.
- **Stay connected:** Ensure that all team members know the best and expected vehicles for communication. Commit with one another to the expected response period as outlined in the employee’s telework agreement. Be as responsive to your direct reports and colleagues as you expect them to be to you.
- **Be transparent:** Use shared calendars, instant messenger and Microsoft Teams meetings as tools to ensure that team members are apprised of one another’s work status.

[Find more tips from GSA here.](#)

Gartner’s New Model for Managing Remote Employees

In response to the COVID-19 pandemic, Gartner developed the NEAR model to help managers work more effectively with remote employees and teams. The model has four steps:

- **Normalize self-direction.** Gartner research has found that two-fifths of remote employees want more self-directed work. The key? Managers must trust their employees and shift from directing their work to coaching them to success.
- **Enable new relationships.** A Gartner survey found that 41% of respondents don’t feel connected to colleagues when working remotely and 26% of employees feel isolated when they work remotely. Managers must learn to recognize when employees feel disconnected and respond quickly.
- **Accentuate the positive.** In a remote work environment, employees are twice as likely to receive corrective feedback vs. positive feedback. Managers need to address that imbalance — and make all feedback evidence-based and forward-looking, Gartner says.
- **Revamp team expectations.** Employees who are working at home still need to see themselves as part of a team. “It is crucial for managers to set expectations with individual team members and the larger team to ensure effective individual contributions and team collaboration,” according to Gartner.



Note to CIOs: Have You Thought About This...?

In a [recent report](#), NASCIO provided some guidelines for responding to the pandemic — and to similar crises in the future. The report highlights several issues that CIOs might overlook:

Make disaster recovery plans pandemic-ready

Most disaster recovery and business continuity plans were not written with something like COVID-19 in mind. In its report, NASCIO urges states to update their plans to address the unique problems associated with a pandemic. The revised plan should include:

- A focus on capabilities that are needed in any crisis
- Identification of functional requirements
- Planning based on the different severity levels of a pandemic event
- Service-level requirements for business continuity
- Revisions and updates — having critical partners review the plan
- Storing hard and digital copies of the plan in several locations for security

Factor contractors into your plan

Given their increasing reliance on commercial services, CIOs must think how services might be affected if their contractors have many employees sidelined by illness. They especially need to stay updated on the status of cybersecurity contractors, the report states.

Manage customer relationships

In this case, the “customers” are the internal agencies that an IT department serves. Given the challenges of a largely remote work environment, CIOs “need to have conversations with agency business partners about disruption to manage expectations and answer questions about rates and service level agreement provisions,” the report states.



4 Lessons in Building Organizational Resilience

Julia Richman, Chief Strategy Officer at Colorado's OIT, recently wrote a [blog post](#) reflecting on how organizations can use their experience with the COVID-19 pandemic to increase their resilience going forward.

Here are the lessons that she shared:

- **Never waste a crisis:** “Change can actually be easier in times of disruption,” she wrote. “Use this time to push more heavily on existing critical investments in cloud, collaboration and redundancy tools.”
- **Teamwork is everything:** She notes that research has found that people are more likely to survive a disaster if they know their neighbors. “I like to think that anyone can be our neighbor and that even in social distancing, staying connected to one another will help us work through any obstacle.”
- **Work can get done under any condition:** Do you feel less productive working at home? If so, you might be working too much. As surprising as it sounds, people often are more productive when they take small breaks “for things like sick kids or making lunches, rather than staring endlessly at your computer screen,” Richman wrote.
- **Learn from everything:** “Even as emails and deadlines are flying, the pressure cooker we’re in right now can be really informative as to future shocks and stresses on our systems, tools and teams,” she wrote. “Take some time to jot down your observations, opportunities for improvement and new ideas that come from these challenges. You might not be able to take action yet, but eventually you will!”

Conclusion: Is Resilience the New Normal?

The COVID-19 crisis has raised several important questions about the future of government operations.

One question is about the future of telework: Given the general success of the remote work environment, will agencies allow more employees to telework, or allow them to telework more often? That remains to be seen.

Another common question is about the role of the CIO and IT department in their respective agencies. IT certainly demonstrated its value in helping agencies cope with the disruptions of remote work. Going forward, will IT leaders be treated as key stakeholders in their agencies, where some are now viewed as playing a supporting, not strategic, role? Again, that remains to be seen, although IT made a strong case for itself.

And then there's the matter of resilience. There's no question that agencies need to leverage lessons learned during COVID-19 to make their operations more resilient. The question is how to do that. How can agencies ensure that a future crisis will not disrupt either their internal processes and workflows or the services that they provide to the public?

Resilience is not a new idea. It's the underlying principle of continuity of operations and disaster recovery planning. But in the wake of COVID-19, agencies are thinking beyond disaster-like scenarios. The question now is this: How can agencies reengineer their operations and services to run seamlessly no matter where employees are working?

In many ways, what agencies are talking about is digital government. By moving to modern workflows and business processes, they have the opportunity not just to improve their resilience but to end up with more cost-effective and efficient operations.

Which brings us to a final question: Having seen what's possible with digital government, how could agencies settle for anything less?



About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the Master Government Aggregator™ for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow [@Carahsoft](https://twitter.com/Carahsoft), or email sales@carahsoft.com for more information.

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](https://twitter.com/govloop)

Thank You

Thank you to Adobe, BlackBerry, Carahsoft, Gigamon, Okta, Rapid7, Red Hat, ServiceNow and SolarWinds for their support of this valuable resource for public sector employees.

Author

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

Designer

Kaitlyn Baker, Creative Manager

Carahsoft's telework, collaboration and cybersecurity solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, NASPO ValuePoint, and numerous state and local contracts. Learn more at Carahsoft.com/Count-on-Carahsoft.

See the latest innovations in government IT from Carahsoft's vendor partners at Carahsoft.com/Innovation.



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

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com

@GovLoop

