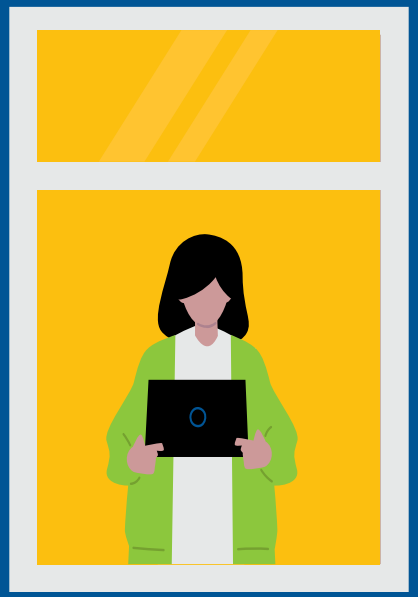
The Connected Employee

Ensuring the Security and Resilience of Government Operations



GOVLOOP
E-BOOK
2020

Executive Summary

Not long before the outbreak of COVID-19, a research report on global work trends made several predictions about the future of work:

- The growing availability of mobile access will enable much of the workforce to work almost anywhere.
- Workers will demand workspaces with far greater mobility and remote access.
- The proliferation of mobile workforces will force organizations to rethink the way they protect networks that enable the connectedness of far-flung workers.

In the future, the report suggested, mobility and flexibility will make it possible to fundamentally reimagine the way workers work. A new kind of worker, the connected worker, will emerge – but only if the systems that connect people are resilient and secure.

Well, the future is now, and it seems to have arrived overnight.

Amid the recent crisis, the world of work has changed in sudden and dramatic ways, including shifts that are challenging the security and resiliency of workplace infrastructure. Tens of millions of people in the United States and hundreds of millions abroad have abandoned offices to work from home and other remote locations. Legions of displaced employees who until recently had never heard of Zoom are attending or hosting online teleconferences. Dining rooms have become boardrooms. And workers have learned to pair sweatpants and a collared shirt to dress for success.

And that research report on the future of global work trends? It nailed its predictions – with one exception. The emergence of large-scale flexible workplaces and mobile workers was supposed to evolve in a somewhat orderly fashion, over years if not decades. That didn't happen, of course, and now government organizations are trying to understand and deal with the aftermath of the pandemic and encroaching economic recession that could result in smaller government budgets.

A vision is emerging of a new kind of flexible workplace, one in which people do their jobs wherever they are – without losing productivity or compromising security. It remains to be seen whether traditional offices will go the way of typing pools, time clock cards and three-martini lunches. Whatever happens, governments at all levels have a duty to continue pursuing public service. Agencies must enable the productivity of workers – wherever they are – by providing workplaces that are resilient and secure.

Contents

In the News

If necessity is the mother of invention, COVID-19 might be the mother of workplace reinvention.

Consider the sudden and massive scale-up of teleworking at federal, state and local agencies. When the pandemic emerged, governments enacted large-scale social distancing measures and other interventions intended to slow the virus. Subsequent disruptions of economic activity and workplace routines have led to Depression-era levels of unemployment, business failures and the mass migration of workers, from offices to home offices. The speed and scale of workplace disruption is unprecedented.

Amid the upheaval, government agencies and other organizations that manage large workforces have begun to see a glint of hope against the backdrop of despair. The pandemic created conditions in which tens of millions of people were unable to assemble at traditional workplaces, forcing employers to find new ways of doing business. Most significantly, it has catalyzed acceptance of flexible workplaces in government agencies, something that would have been inconceivable a few months ago.

"It really caught everybody off guard," said Allen Shark, Executive Director of Public Technology Institute, a government technology advocacy group. Governments' disaster recovery plans, which in retrospect were wholly inadequate, "contemplated having to be away from an office for a couple of days, maybe a week or two, but certainly not this mass migration towards telework," he said.

Transitioning into a poorly understood "new normal" hasn't been easy, especially at its onset. Government agencies bungled the disbursement of stimulus checks and small business loans. Record numbers of unemployment claims overwhelmed the capacity of states to process them, resulting in crashed systems across the country. "Hardest hit were local governments, because that's where people conduct most of their business," Shark said.

Digital Collaboration Tools in High Demand

Agencies responded to the challenges by taking action to reconnect with displaced workers. In what amounts to a large-scale technological relief effort, federal, state and local governments provided access to laptops, headsets, broadband hotspots, upgraded internet service and communications apps – whatever it took to transform marooned workers into connected employees.

Planning for large-scale disruption inevitably falls short because disruptive events rarely conform to expectations. During the Cold War, the country built fallout shelters to survive atomic bombs that never fell. In the leadup to the year 2000, the world braced for a Y2K IT disaster that didn't materialize. Conversely, few people envisioned or prepared for the Sept. 11 terrorist attacks. When responding to an unanticipated event, it helps to be flexible. When government responds to a disaster, having a flexible workforce is essential.

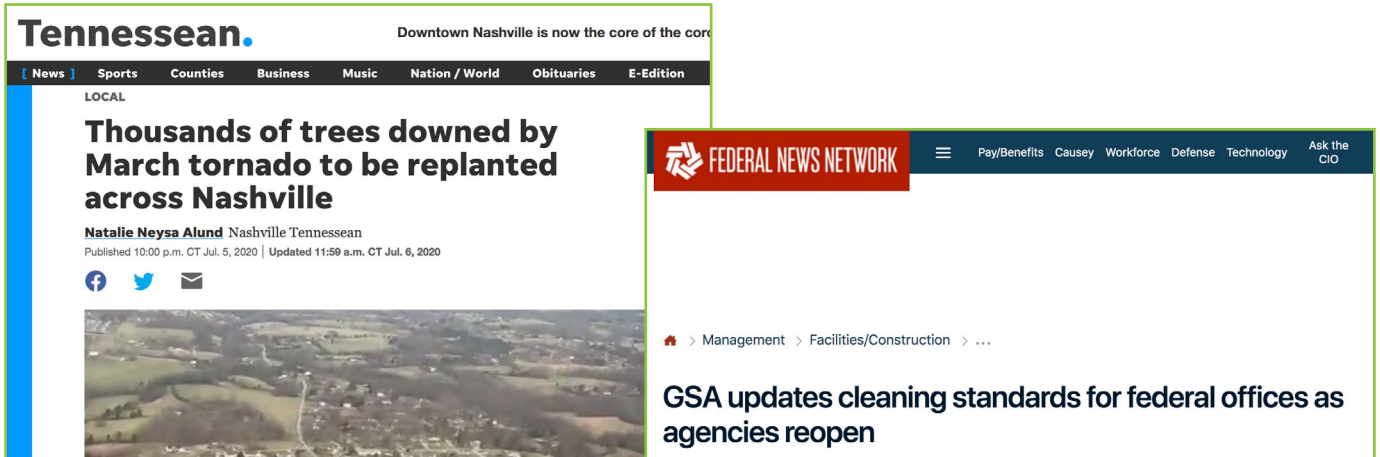
The General Services Administration (GSA) was better prepared for the pandemic than some agencies, in part because of an ongoing initiative to foster a "communicative culture" that permeates the agency and its workers, regardless of what they do or where they sit. During this recent crisis, that culture has served GSA well.

"Open communications in person, via email, via chat, via video, via all those mechanisms was just kind of the norm, so when we switched over in response to the national emergency, it wasn't a big change for how we operated," said David Shive, GSA's Chief Information Officer.

State governments face similar challenges of how to manage and communicate with employees who are no longer working in traditional offices. In Tennessee, on March 3, two days before the state announced its first case of COVID-19, a tornado with winds of 125 miles per hour ripped across the state, passing just north of the state Capitol. Government buildings lost power, and the state's data center relied on emergency generator power for several days. Many state employees were told to work from home.

"That was sort of a dry run for the pandemic," said Stephanie Dedmon, Tennessee's Chief Information Officer.

Using a combination of collaboration tools and modified management protocols, Tennessee's public sector workers have remained connected and adjusted to the challenges of the pandemic. "You have to make an extra effort as a supervisor or manager to reach out and make sure that your employees feel connected," Dedmon said.



Cyberattacks on Government Agencies

Even as governments at all levels moved to institute flexible work arrangements, cyber attackers sought to take advantage of disruptions.

In March, cyber attackers tried to overwhelm servers at the Department of Health and Human Services Department with millions of hits. The campaign of disruption and disinformation was "aimed at undermining the response to the coronavirus pandemic and may have been the work of a foreign actor," according to Bloomberg.

In April, NASA released a memo warning that federal agencies' newly transitioned teleworkers were the targets of "a new wave of cyber-attacks."

In May, the Red Cross urged an end to cyberattacks against health care organizations, including attacks against hospitals and attempts to infiltrate medical research centers and steal data about COVID-19 treatments, Reuters reported.

Lessons learned from Texas in 2019

At every level of government, organizations have found innovative ways to communicate among staff during the pandemic, including the use of teleconferencing platforms and messaging apps to connect with disconnected workers.

Prior to the crisis, many workers hadn't used or heard of tools that have become workplace lifelines. "Knowing that the business of government must continue, they found innovative ways to communicate," Shark said.

At times, the crisis has been an impetus for enacting long-overdue upgrades, such as jettisoning the reliance on paper records and adopting digital work processes. "Many of these governments knew that at some point they would need to convert, but they thought they had more time," he said.

For years, many managers worried that employees working outside the confines of an official office would slack off and shirk responsibilities, despite research suggesting otherwise. Recent anecdotal evidence reinforces the notion that remote workers are as productive as their office-bound counterparts, if not more so. The finding suggests that managers might be open to even more flexible workplaces in the future.

"The idea of having a flexible workforce that's productive has been proven," Shark said. "It took a crisis to show that telework is incredibly important and legitimate. Telework has been legitimized, finally."

"People are more productive," Dedmon said. "They're getting more done. Even some of the biggest naysayers about work from home are seeing that it can work. I think this new normal will involve a lot more of us working from home. Coming into the office will be the exception."

Need to Know

The ABCs of a Connected Workforce

A large-scale workforce migration, from traditional offices to flexible workspaces, is a complex undertaking – like moving on-premises, legacy IT systems to the cloud. There's much more to it than a simple lift and shift.

Executing an effective transition is a process of making myriad tweaks and adjustments that affect multiple systems up and down the chain of operations. The transition affects all levels of an organization. As with most complex endeavors, it pays to start with the foundation.

Tsedal Neeley, a professor of business administration at Harvard Business School, said the first order of business for organizations making a major shift toward remote work is to "get the infrastructure right." To ensure that every employee has access to critical work tools, Neeley told the Harvard Business Review, leaders must answer critical questions that get at the practical dimension of enabling connected workers:

- Do people have the requisite technology or access to it?
- Who has a laptop?
- Will they be able to easily access the organization's network?
- Will they have the software they need to do their work, have conference calls, etc.?
- How many employees don't have laptops or mobile devices?
- How do you ensure they have necessary resources?

Navy Keeps Security Front and Center

The size of an organization will influence how it sets up connected workers to be successful. Some large federal agencies have encountered and overcome barriers to connectivity that might not present challenges to smaller organizations.

The U.S. Navy, for example, has simultaneously striven to manage the pandemic's impact on the health of its workforce and its information systems. On March 22, a sailor on the USS Theodore Roosevelt aircraft carrier tested positive for COVID-19, the first of more than 1,100 reported cases of infected crew members on that vessel. On March 27, the Defense Department began rolling out a temporary cloud-based platform to relieve pressure on existing networks strained by the surge in remote workers. The system integrates with Microsoft Office 365.

"During this international health crisis, we are teleworking in unprecedented numbers, which has placed a greater demand on the Navy's infrastructure," a Navy spokesman said.

The Navy stressed that security is a key concern. The temporary platform, known as Commercial Virtual Remote (CVR) environment, will only handle unclassified information. Users must migrate critical documents and official records to an approved storage platform. If a government-issued command access card (CAC) reader is used on a personal computer at home, the reader isn't allowed to be used with a government-issued computer.

"Getting the job done at the expense of information security is unacceptable," said Vice Adm. Matthew Kohler in a written statement.

VA Builds on Digital Transformation

The country's second largest federal agency, the Department of Veterans Affairs (VA), has responded to the COVID-19 pandemic by distributing more than 16,000 laptops and 7,500 iPhones. An additional 250,000 laptops are on order to accommodate workers who previously didn't have mobile devices, and to upgrade older equipment.

VA's remote workforce of approximately 140,000 people is several times larger than the 30,000 or so employees who worked remotely before the pandemic. The agency has doubled its bandwidth capabilities and tripled its capacity to deliver telehealth. Between January and May, the number of daily patient telehealth visits increased from 2,000 to more than 25,000.

During the pandemic, VA has turned to apps to smooth its workflow and the delivery of services. The WebEx teleconferencing tools has added 16,000 new VA accounts since April 1. The agency's VEText Team developed the "I Am Here" app, a secure messaging system that lets vets use their phones to remotely check in for appointments. Use of the Annie App for Clinicians is growing. In response to COVID-19, VA created its first customer-facing chatbot. Other apps are in development.

"Since the COVID crisis broke … we expanded our capabilities in weeks, doing things that would typically take us months or even years," said Dominic Cussatt, VA's Deputy Chief Information Officer, speaking at an industry event in June. "We really scrambled and looked at what our customers needed and got the remote work and remote capabilities in place."

VA's ability to respond to the crisis and field a remote workforce benefited from a digital transformation initiative undertaken by the agency four years ago. During that time, VA has focused on improving customer service, IT modernization, strategic sourcing, IT workforce transformation, and secure and seamless interoperability. "A lot of the digital transformation work we did to create a virtual cloud environment has paid off," Cussatt said.

The payoff includes enhanced security at a time when some cyber attackers are trying to take advantage of workplace disruptions caused by the pandemic. Through April, the agency has "already blocked in the hundreds of millions of malware attempts," Cussatt said. "And we have at any given time … 45 or more prioritized cybersecurity projects to up our game and increase our cybersecurity posture."

Six Steps to a Mobile Workforce

1. Alert and Notify: Use whatever means necessary – email, Facebook, Twitter, local media, etc. – to let everyone know that government will continue to operate, albeit differently.
2. Establish Online Strategies: Confirm that remote workers have the tools, especially communications tools, to be productive. Check IT systems for resilience, security and remote management.
3. Leadership Communications: Equip elected leaders and senior staff with tools for conducting business using video conferencing and other web-based technologies.
4. Application Review: Where possible, move site-based services, such as permitting, to online platforms.
5. Reaching the Unconnected: Find ways to engage the 19% of Americans who don't have direct access to broadband or online services.
6. Review, Train, Practice: Anticipate closure of facilities. Review current plans and improve business operations.

Source: CompTIA

Building Blocks

In the flexible workplace that continues to emerge, the role of workers will change in profound ways. Under the traditional work paradigm, employees used resources accessed on networks to do their jobs. The connected employee, by comparison, will be a part of the network – not apart from it. Untethered from an office workspace, the connected employee will function as a critical node in a tightly integrated IT system.

Four key elements inform the connected employee: connectivity, engagement, productivity and collaboration.

Connectivity and Security

Above all, the connected employee must become part of the enterprise in a way that is stable and secure. Connected employees will agree that:

"I am part of the same enterprise with other folks, with access to the information and systems I need and able to collaborate securely and effectively, technologically speaking."

Achieving this goal at scale will be a challenge. In April, a survey by Gartner indicated that 41% of employees are likely to work remotely, at least some of the time, after the COVID-19 pandemic. By June, Gartner had raised the projection for post-pandemic remote workers to 48%.

"The biggest change that will occur is a much more hybrid world where some employees are working from home some of the time," said Brian Kropp, Chief of Research in the Gartner HR practice. He said organizations must invest in new HR systems, technology and processes to support connected employees. Until now, that support has largely existed as an ad hoc approach, he said.

To that end, agencies must provide employees with IT tools needed to perform work, being ever mindful of providing security in their workloads. The starting point for secure connectivity is the combination of cloud and endpoint management – providing ready access to applications and data, while ensuring that the endpoints don't put those resources at risk.

Security concerns cover a range of activities, from secure access of systems and applications from remote locations to the deployment of secure collaboration tools. But the foundation of secure connectivity is the combination of cloud and endpoint management.

The U.S. Agency for International Development (USAID), for example, protects its external systems by enforcing strict controls, including two-factor identification, virtual desktop functionality and a suite of information security tools: data loss prevention, log monitoring and a cloud access security broker (CASB). The VA has apps that benefit employees and customers, including the agency's first customer-facing chatbot.

Productivity

The performance of remote workers during the pandemic has disabused some skeptics of the notion that employees who work away from the office might be less reliable. Flexible workplaces nonetheless have challenges that might not be a problem for a traditional office. Managers must be vigilant to ensure that connected employees can state, without reservation, that:

"I have the tools I need to not just meet compliance, but to work productively."

For an agency such as USAID, with 80 overseas locations, ensuring the productivity of connected workers is a matter of "having IT services and products that balance the need for transparency – that business-driven gathering and sharing of information – with the need to keep that information secure," said Jay Mahanand, USAID Chief Information Officer (See the full interview, Page 15).

At security-conscious organizations, protecting IT assets is at least as important as productivity, which is "essential for continuing to deliver our work," Mahanand said.

As workplaces evolve and the connected worker becomes prominent, the concept of productivity will change, too. "We've had to develop new norms for our cloud collaboration tools, such as guidelines for hosting an effective online meeting, and evaluate new platforms that are accessible for larger audiences or in countries with underdeveloped infrastructure," Mahanand said.

Engagement

For some workers, traditional offices provide a sense of place and purpose that keeps them engaged. Absent those physical structures and proximity to team members, some workers can become estranged. A connected employee will agree with the proposition that:

"I feel like I am part of a team, seeing my own work as part of a larger mission."

Agencies and their leaders have a responsibility to engage and re-engage with employees – and to make sure those employees understand that their work is meaningful. Many managers said the overnight emergence of large-scale remote and flexible work arrangements effectively ended business as usual. Out of sight doesn't mean out of mind. It means that managers must double down on engaging connected employees.

"We encourage constant feedback and check-ins with employees. I always like to say we over-communicate. … We build a two-way communication with them to make sure that happens," Shive said. "One of the things that keeps them engaged is clearly laying out what our goals and responsibilities are for our organization and expressing to people what their part is in that."

In Colorado, remote workers receive a "tech kit" that offers guidance on equipment, getting tools to work, internet access, phones and other issues. "We do not want employees plugging personal computers into our state network," said Theresa Szczurek, the state's Chief Information Officer. "Security in this time is very, very important."

During a time of massive workplace disruption, leaders deliver tremendous value when they "find ways to motivate people," Mahanand said. "Foster an environment where people want to come to work every day, whether that workplace is an office or on a virtual platform," he said.

Collaboration

Automation, artificial intelligence and other advanced technologies will continue to do more of the mundane and repetitive tasks that human workers once handled. Relieved of those responsibilities, workers will devote more of their time solving higher-level problems. Frequently, solving those complex challenges requires the attention of highly collaborative teams. The connected employee agrees that:

"I'm able to collaborate in a way that leads to new and better ideas."

Nurturing collaboration among connected employees in a flexible work environment can be a challenge. Employees working remotely can become isolated and suffer from not having unplanned interactions with colleagues, such as when colleagues chat in the hallway, that spark creativity and collaboration. To offset those liabilities, agencies are encouraging employees to be creative in the remote environment.

More than two in five workers have reported not feeling connected to colleagues, according to Gartner. Organizations are responding by increasing communication with workers and encouraging managers to do more outreach, Kropp said. In addition, some workers respond to flexible work arrangements by working more hours, which can lead to burnout on top of isolation. Some organizations have responded by increasing personal time off.

Since the development of its first mobile-enabled workforce, GSA has measured outcomes of connected workers. The data shows that mobile workers are productive, and that they connect as much as they need to if they have the right tools. GSA's experience also found that mobile workers miss out on opportunities for spontaneous interactions with colleagues that promote collaboration. GSA offsets that effect by getting workers together for virtual team coffees and lunches.

"[We try to] generate some intentionality around building collaboration at intersection points between teammates that are more than just sending an email or something like that," Shive said.

Industry Spotlight

Remote Work Requires Rethinking the Endpoint

An interview with Tommy Gardner, Chief Technology Officer, HP Federal

Like most things, working from home has pros and cons. Employees might get to sleep a little longer or get back hours of their commute time. They also face new security threats that lurk inconspicuously in their home IT environments.

Dr. Tommy Gardner, Chief Technology Officer at HP Federal, said endpoint security is the problem he is most concerned about in the work-from-home environment. "I'm most worried that your home network, which is the internet connections you have, the router and your endpoints, are not going to be at the same protective cybersecurity level as what you would have in government, in a well-protected, well-diagnosed network environment for the agency,"

The recent pandemic has revealed how essential digital transformation is and agencies have begun to accelerate the process of modernizing IT. We spoke with Dr. Gardner to learn more about how agencies can modernize and strengthen their IT environments, when employees are working from new and remote locations.

Think in Terms of Risk

Exponentially larger percentages of government employees are using virtual private networks, or VPN, to stay secure. These fall short of securing employees' endpoints, such as laptops or mobile devices, which remain vulnerable.

Consequently, agencies need to take a risk-based mindset more than before. They have to acknowledge that with more endpoints, there are new risks, and bad actors will take advantage of this.

"You have to believe that the advanced, persistent threat, or the enemy out there on the dark web attacking networks every day, is going to focus on attacking employees in their home environment," Gardner said.

Think About Endpoint Management

To tackle the new threats in the home environment, endpoint management is key.

"Remotely managing endpoints is a capability you would want as a chief information security officer or chief information officer in an agency. You want to be able to have insight into what's going on in your machines. Do they have the right updates? Can we push the right updates to them? Do we have the right protection?" Gardner said.

Many agencies are migrating their data management to the cloud. But especially when employees are working from remote locations, there can be numerous endpoints accessing the cloud on systems that are not secure. So, in order to really elevate endpoint protection, agencies need to consider the security of the devices themselves.

Think About Printers as The Weakest link

Printers are one kind of endpoint that can introduce a host of security risks in the home environment.

The printer, often an insecure endpoint, becomes the inconspicuous entryway for hackers to break into a network and access high-level, confidential information. Few printers were designed for top-level cyber protections.

"Agencies' cybersecurity is only as strong as the weakest chain in the network," Gardner said. That's why printers that come with built-in security can offer more layers of protection. By having embedded security at endpoint machines, agencies can strengthen their line of cyber defense.

HP PCs and printers come with built-in security solutions that protect from firmware attacks, malware, phishing and other threats that have only grown more common during the global pandemic.

"At HP, we design our printers with the same philosophy and architecture that we design in our personal systems, workstations and laptops, which is world class cybersecurity," Gardner said.

Your mission is our mission.

Get outstanding reliability, security, and innovative design with HP. HP creates technology specifically configured for government agencies. Through our portfolio of printers, PCs, mobile devices, solutions, and services, we provide the technology that will help your agency maximize its public benefit.

Learn More

Thought Leadership

Tennessee Keeps Workforce Connected, Mentally Healthy

The pandemic and its repercussions have magnified the importance of mental health. The crisis has accelerated a kind of workplace where anyone can work from anywhere. But it has also unveiled the need to help isolated, distributed employees stay mentally healthy.

"I think we're realizing that the mental aspect of this pandemic is something that we need to address and not ignore," said Stephanie Dedmon, Chief Information Officer for the state of Tennessee.

It takes both individual and enterprise actions to help employees be mentally healthy. In a recent GovLoop interview, Dedmon spoke about her efforts as an IT supervisor to keep her team mentally healthy, as well as the government's actions to provide tools and extend flexibilities in a time of crisis.

The following interview was slightly edited for clarity and brevity.

When it comes to the workforce being and feeling connected, how does an office compare to remote work?

Our state has had a formal work-from-home process for a number of years. My team has worked hard to provide all of the appropriate collaboration tools that enable a person working from home to 1) do their job and be productive and 2) stay connected. But what we find is that you have to make an extra effort as a supervisor, as a manager, to reach out and make sure that your employees feel connected. I think the challenges are just making sure that you make time for that.

If I don't have a scheduled call with my direct reports, I try to reach out by phone, by email, and ask, "How are you doing? What's going on this week? How can I be helpful?" I think we're recognizing that the mental aspect of this pandemic is something that we need to address and not ignore. We need to make sure that we check in on people more frequently than we might normally.

Have there been any agencywide initiatives around employees' mental health?

We've shared webinars on stress and mental health with the workforce. Like so many things, I think verbalizing and recognizing that it's a struggle — and we're all struggling in different ways — is important. In this day and age, we have to talk about it, recognize it and make sure we give people tools and access to additional help.

We've leveraged our employee assistance program to provide things like noontime yoga or energizers. We encourage people to schedule those with your team, whether that's a group of five or 20. Be purposeful in putting that on the calendar, encourage people to attend remotely, and spend 15 or 30 minutes in something that's not work-related, that physically helps people refresh and do something besides sit at their desk and talk to their computer.

How has the agency approached working with employees who have to care for children at home?

Something that our enterprise Department of Human Resources did — I think at the governor and his leadership team's suggestion — is that we relax requirements, knowing that clearly, many people have children at home.

As part of our formal work-from-home program, it wasn't really acceptable to say that you don't have childcare and work from home while you have children at home. But we have relaxed that requirement and formally asked supervisors to be more flexible on people's schedules. Allow people to work when they can, and when they need to care for children or be teachers, as the case has been, make sure employees understand that's OK. That we trust them, and we want them to be able to do what they need to do for their families.

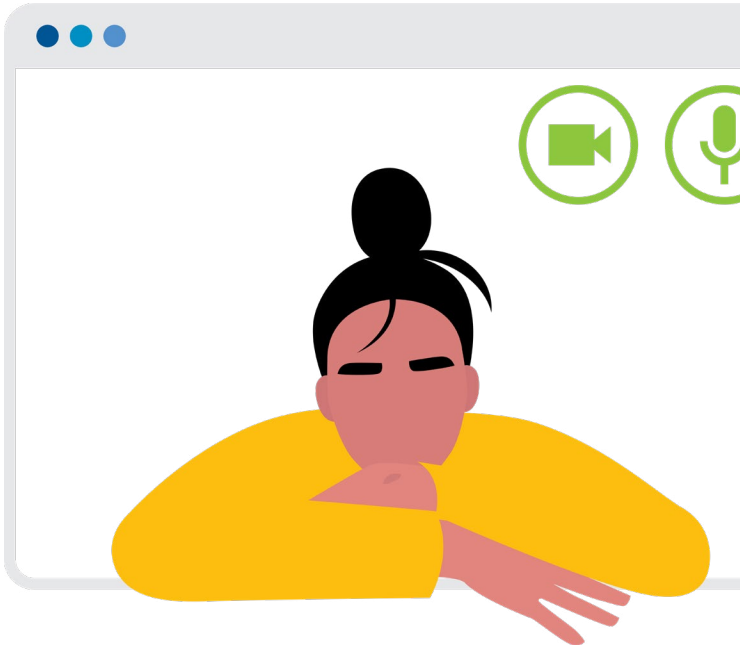
Have you seen employees able to take advantage of this flexibility?

I personally know some of our employees who are. [For example, one employee] works in the morning, and then at lunchtime, she switches off [with her partner].

I've been amazed at the creativity that some of our employees are reaching in terms of trying to make it all work. I personally don't have young children at home, and I say an extra prayer for those who do. Because that adds in another layer of stress and mental taxation that we need to recognize that our employees are dealing with.

What kinds of factors can you attribute to employees being resilient and staying engaged in their work?

I'm not sure that I can necessarily put my finger on it. Not to minimize the impact that the tornado had on middle and east Tennessee in early March, but we occasionally joke that that was a dry run for the pandemic that was to come. I think, honestly, having gone through the tornado, a lot of our folks were like, "OK, we've dealt with that. Now we can deal with the pandemic."



Thought Leadership

USAID Makes Productivity a Priority

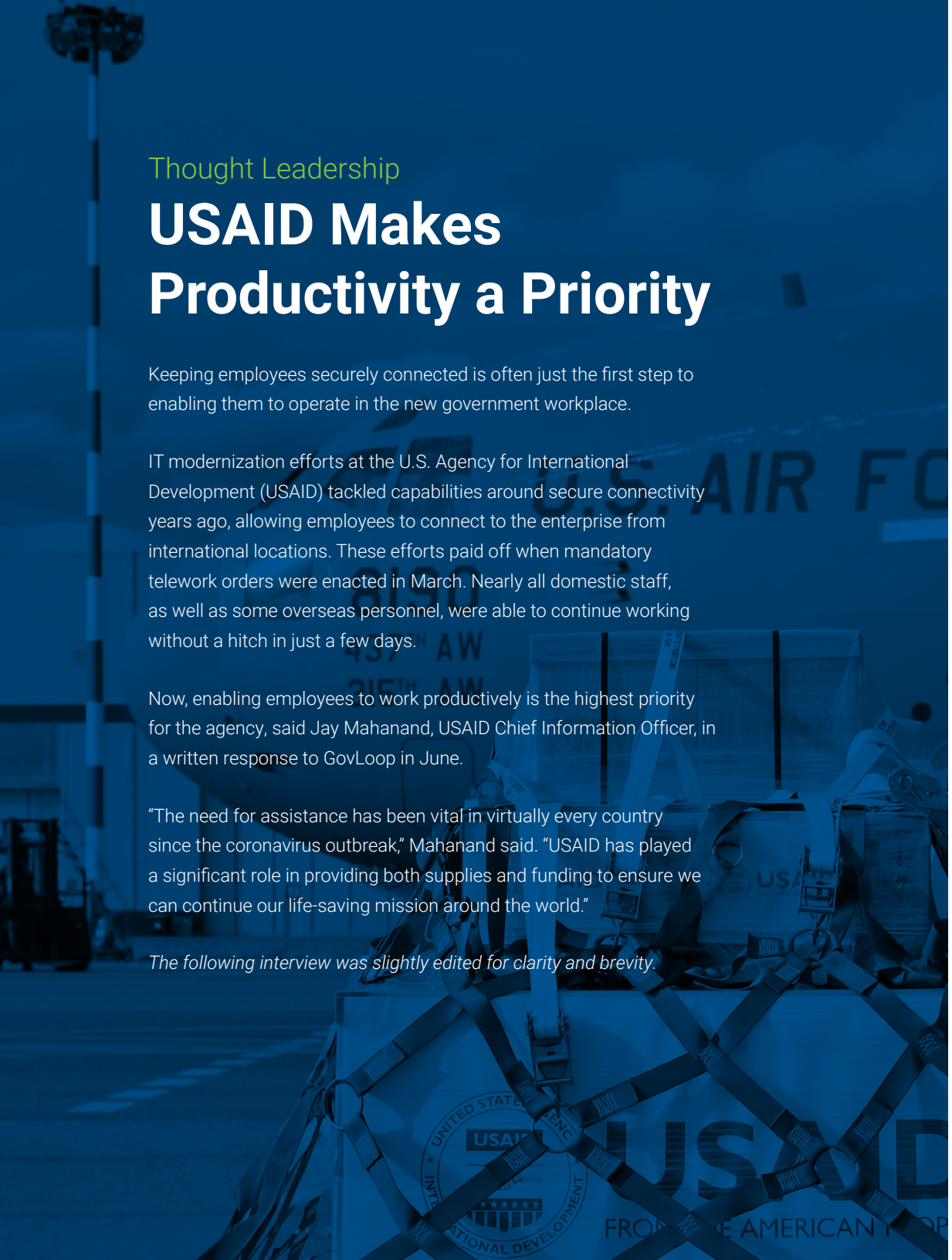
Keeping employees securely connected is often just the first step to enabling them to operate in the new government workplace.

IT modernization efforts at the U.S. Agency for International Development (USAID) tackled capabilities around secure connectivity years ago, allowing employees to connect to the enterprise from international locations. These efforts paid off when mandatory telework orders were enacted in March. Nearly all domestic staff, as well as some overseas personnel, were able to continue working without a hitch in just a few days.

Now, enabling employees to work productively is the highest priority for the agency, said Jay Mahanand, USAID Chief Information Officer, in a written response to GovLoop in June.

"The need for assistance has been vital in virtually every country since the coronavirus outbreak," Mahanand said. "USAID has played a significant role in providing both supplies and funding to ensure we can continue our life-saving mission around the world."

The following interview was slightly edited for clarity and brevity.



What does the workplace look like for USAID employees?

The majority of USAID's staff are in a traditional office-type setting. However, USAID has more than 80 overseas missions [locations] and have staff who are out in the field or are mobilized to crisis locations when needed.

How does this new government workplace where more people are able to work from anywhere change how the workforce is connected to the agency enterprise?

For USAID, it isn't significantly different. As an international organization, and given the global business demands of how USAID delivers foreign assistance on the ground, staff are already heavily reliant on modern, mobile IT solutions.

More than 10 years ago, USAID began a significant IT modernization effort that provided staff with [capabilities such as] real-time access to data, applications that support different endpoints and accessibility to social collaboration tools to gather and share information that supports informed programmatic and business decisions.

These early modernization efforts enabled USAID to have nearly all U.S.-based staff, as well as a good portion of our overseas staff, up and running within the first few days of the mandatory telework order in mid-March.

How can agencies enable employees to be securely connected to their enterprise? What kinds of IT capabilities have you used to address this?

For USAID, it's about having IT services and products that balance the need for transparency — that business-driven gathering and sharing of information — with the need to keep that information secure.

The agency maintains strict controls for accessing its primary external systems via two-factor authentication, virtual desktop functionality and a suite of information security tools including data loss prevention, log monitoring and a cloud access security broker (CASB).

Taking it a step further, how can employees work productively from wherever they are? Secure connection is the first step, but what kinds of capabilities and strategies have you implemented for employees to work effectively?

Change management has been an important part of moving a significant portion of our staff to working remotely on a full-time basis. The agency already had crisis management, risk management and disaster recovery baked into its business strategy. However, putting those continuity plans into practice meant ensuring that we are using change approaches to help our staff become more comfortable with new ways of working.

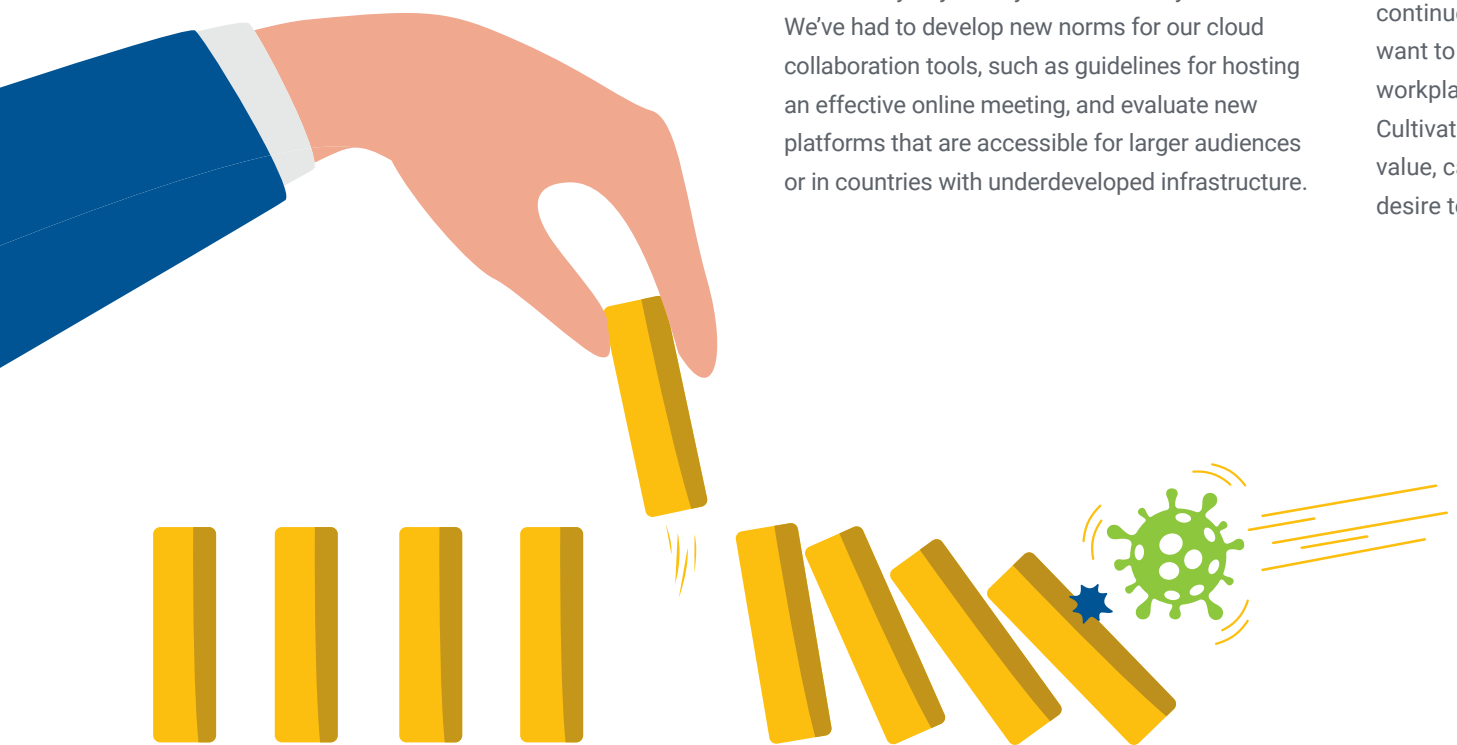
Our change management activities also had to take into account that productivity — which is the work we do every day — may look differently than before. We've had to develop new norms for our cloud collaboration tools, such as guidelines for hosting an effective online meeting, and evaluate new platforms that are accessible for larger audiences or in countries with underdeveloped infrastructure.

Of the four pillars — connectivity, productivity, engagement and collaboration — which is biggest priority to you now and why?

Although all four pillars are critical, particularly in the current environment, productivity is essential for continuing to deliver our work. The need for assistance has been vital in virtually every country since the coronavirus outbreak. USAID has played a significant role in providing both supplies and funding to ensure we can continue our life-saving mission around the world and support partner countries in their response to COVID-19.

What is one piece of advice you would give other government leaders to keep employees connected?

Find ways to motivate people. It's important to continue to foster an environment where people want to come to work every day, whether that workplace is an office or on a virtual platform. Cultivate a workplace where staff understand their value, can put their expertise to work and have a desire to continue to grow and learn.



Conclusion

Workplaces and workers have experienced a massive disruption at all levels of government, and almost no one anticipates a return to the way things were. Some of those newly minted remote workers may never go back to the office. And if they do, they could be splitting time between traditional and flexible workplaces.

Whatever happens, systems developed to support connected workers must always be resilient and secure.

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

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