Bouncing Back From Crisis

govloop

Affigent
AN AKIMA COMPANY

ORACLE Platinum Partner

GOVLOOP
E-BOOK
2020

Executive Summary

Years before the COVID-19 pandemic, the federal government was moving toward IT modernization. Some agencies progressed quickly, others with caution. Yet they were all on a seemingly clear path to digital transformation. There were no surprises on the horizon.

But the COVID-19 pandemic has changed everything, including the way agencies think about IT systems, modernization and resiliency.

When the coronavirus emerged, President Donald Trump's administration issued a series of stay-at-home guidelines for federal workers. With little warning, the largest mobilization of remote workers in history began without a pre-approved plan. At the same time, agencies began experiencing spikes in pandemic-related activity that stressed IT systems, particularly in areas involving health care, distribution of relief funds, unemployment assistance, and other critical government services.

Agencies were unsure if their IT systems could keep up. Facing unprecedented demands on infrastructure, they scrambled to procure hardware and cloud computing services to support new demand for teleworking and digital services. Faring best were agencies that had worked assiduously toward modernization before the pandemic arrived.

Ultimately, agencies met the challenge. Federal workers continued working, agencies continued operations and the government continued delivering services. Yet keeping the lights on required heroic, ad hoc interventions. Without emergency aid, some agencies would have been in deep trouble. Others learned that the resiliency of IT systems was less rigorous than they had thought.

As the pandemic persists, the path to modernization no longer looks the same. The pandemic has forced agencies to take stock of digital assets and liabilities, including digitally transformative systems such as cloud, to drive mission success. Agencies are striving to understand how they can become more resilient.

This e-book explores operational and IT resilience in the federal government, the role of modern enterprises in promoting resilience and what agencies are doing to become more resilient in the coming years.

Contents

In the News

In March, seeking to slow the spread of the coronavirus, the Office of Management and Budget (OMB) released a memo directing agency leaders to "maximize telework" for federal workers "while maintaining mission-critical workforce needs." The memo provided no details on how to equip millions of feds to work from home.

During the same month, only 57% of federal workers responding to a GovLoop survey indicated that their agency was able to enforce existing security rules and processes in a fully remote work environment.

On March 27, the Coronavirus Aid, Relief, and Economic Security (CARES) Act provided $2.15 billion to the Veterans Affairs Department (VA) in support of increased telework, telehealth and direct delivery of health care services. The VA used the funds to accelerate ongoing modernization plans, including provisioning a cloud environment to scale up inadequate on-premises solutions. The agency also doubled its bandwidth, tripled the number of employees working remotely and increased delivery of telehealth services tenfold.

In addition, the VA identified opportunities for moving applications into the cloud. The department's IT modernization strategy was sound, said Chief Information Officer (CIO) Jim Gfrerer, but "the multiyear plan will have to be examined on a very frequent basis."

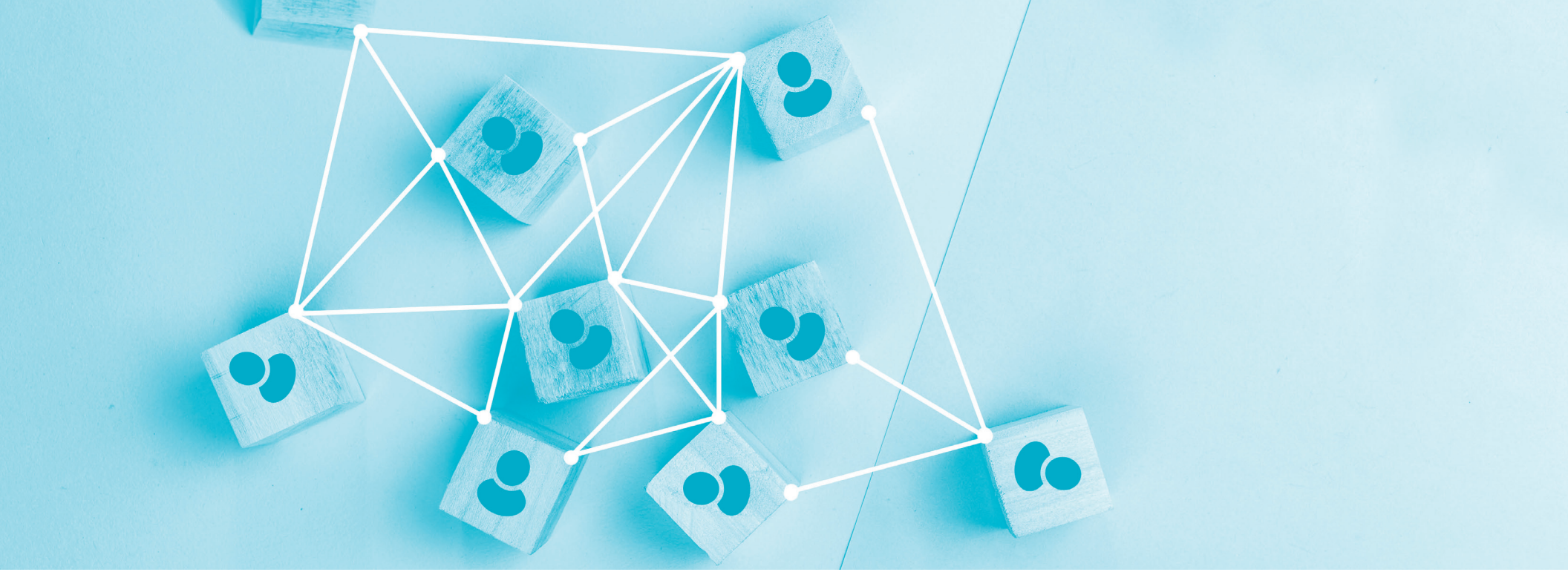
By late March, as agencies responded to the coronavirus, it became clear that past procurement decisions were enabling or impeding current responses. At some agencies, bureaucratic inertia and reluctance to embrace new technologies slowed modernization initiatives and made them less resilient. Since the pandemic began, agencies have been undergoing a "permanent paradigm shift" in the way they view technology adoption, said Kevin Burnett, Pioneer in Residence at the Navy's Naval IX, during a GovLoop forum.

On April 8, amid the surge in telework, the Cybersecurity and Infrastructure Security Agency (CISA) released interim Trusted Internet Connections (TIC) 3.0 guidance. The goal was to help agencies secure network and cloud environments, with a focus on remote federal employees connecting to private agency networks and cloud environments.

By April 10, the surge in telework by Air Force members and employees at other agencies contributed to a 53% spike in virtual private network (VPN) use nationwide, with a projected one-year surge of 150%, according to the Congressional Research Service (CRS). The sharp increase could "stress information communication infrastructure," predicted CRS, noting that it is unclear whether "infrastructure can continue to handle increased loads."

In June, the oversight committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) reported that the pandemic had "strained agencies' networks and shifted IT resources" of organizations that depend on reliable, secure IT systems to perform mission-critical functions. The surge in telework during the pandemic and enlargement of agencies' IT attack surfaces had exacerbated or increased the vulnerability of longstanding challenges: cyberattacks and insider threats, IT modernization, continuity of operations, and a highly skilled cybersecurity workforce.

At the same time, employees at the Housing and Urban Development Department (HUD) reported that the agency was "generally well-prepared"

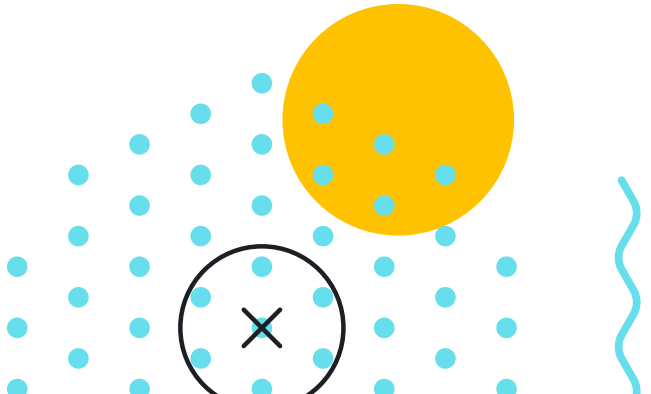


for transitioning to telework. Working remotely nonetheless "severely impeded business processes dependent on paper records or facility access," according to a survey conducted by HUD's Office of Inspector General (OIG). Bandwidth constraints with HUD's IT infrastructure and the lack of government-furnished equipment for some employees further disrupted HUD operations, according to the report.

The pandemic also revealed in June that agencies' employees are more resilient than their technology at times. The Centers for Medicare and Medicaid Services (CMS) pushed its modernization agenda by holding an "upskilling summit" to develop employees' skills in areas such as cloud technology and cybersecurity. CMS's Office of Information Technology (OIT) stood up a new tool that supported teleworkers by remotely monitoring the health of employees' laptops.

Elsewhere, the Air Force reported an acceleration of its digital modernization efforts, expanding VPN access to support telework and improving LTE and 5G commercial connectivity on its bases.

On July 15, a congressional committee heard testimony to consider COVID-19 and its exposure of federal IT's inadequacies and subpar resilience. "While the need to modernize is not new, the pandemic has been a powerful accelerant, turning this chronic problem into an acute, urgent need that demands action," the committee said in a statement, noting that legacy systems receive a disproportionate share of IT funds. "Congress must act to accelerate modernization."



Need to Know:
The ABCs of Resiliency

Resilience is the capacity to recover quickly from difficulties and promptly bounce back. Resilience requires resources in reserve or infrastructure to rapidly access them in times of crisis. Markers of IT system resiliency include agility, flexibility, scalability, responsiveness, speed to solution, mobility, superior analytics, systems maturity, fewer legacy systems, security, and visibility into complex systems.

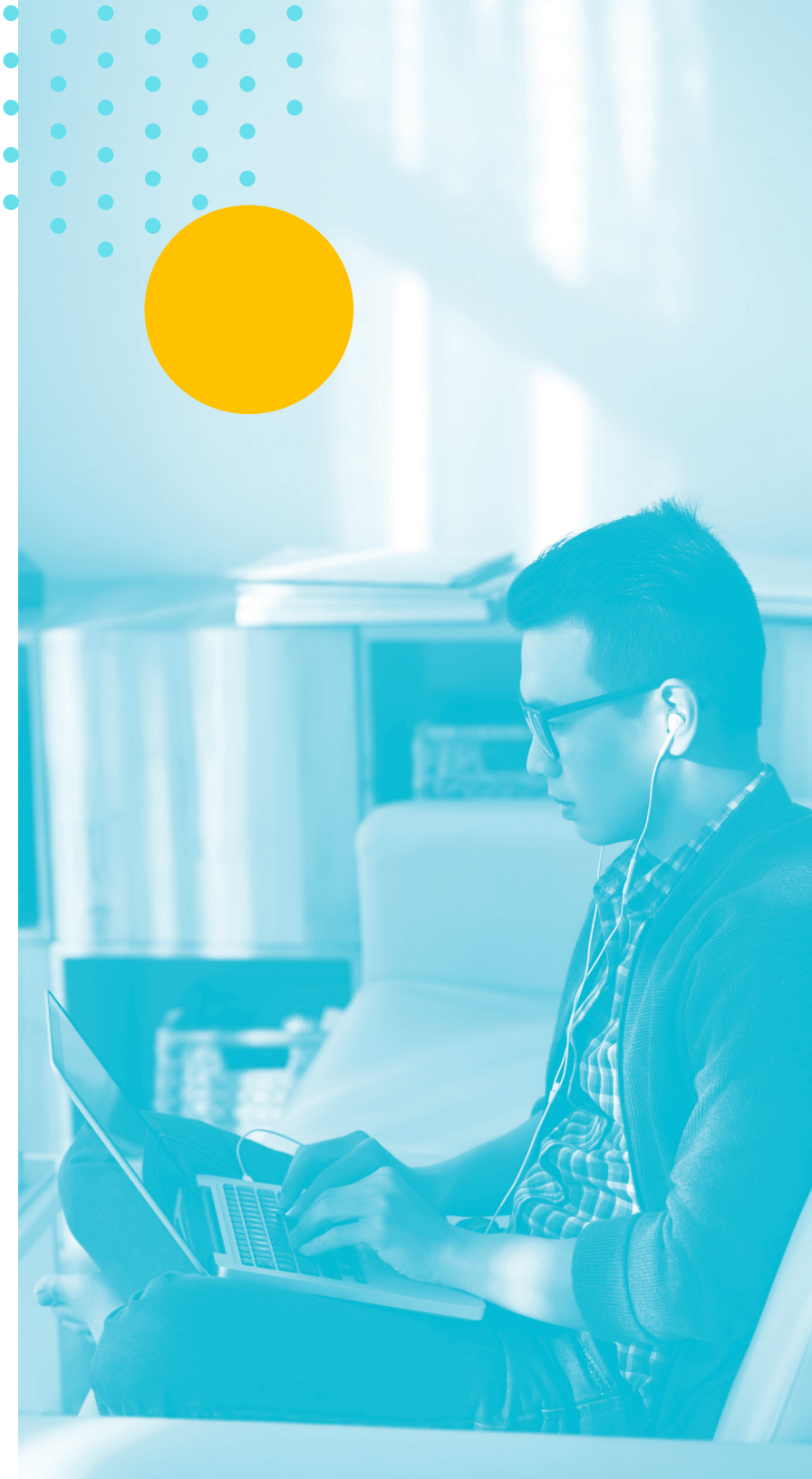
Those features fall into three categories: the ability to adapt, the ability to adjust and the ability to reprocess, said David Knox, Group Vice President for Public Sector Software at Oracle. Oracle is a software company that provides enterprise cloud data solutions.

The Ability to Adapt

Resilient enterprises quickly adapt to shifting circumstances. In government, resilient agencies employ IT systems that are elastic and scalable. When the environment changes, resilient systems absorb new information and execute appropriate responses. Less resilient organizations tend to react (or overreact) to crises, often taking actions that deviate from normal business practices.

When the pandemic made it necessary for federal employees to work at home, the government directed agencies to quickly scale up their remote workforces. Agencies that had taken significant steps toward modernization were able to accommodate the request more easily, with some likening the transition to flipping a switch.

Before COVID-19, the Small Business Administration (SBA) had already stood up a lot of cloud-based capabilities, issued mobile devices to workers, and was moving toward software-defined networking in a wide area network (SD-WAN). Collectively, those upgrades made it easier to "add more capabilities very fast," said Deputy Federal CIO Maria Roat this summer. "The staff was there. The vendors were there … and they really came through when we needed them to."



The Ability to Adjust

In addition to being agile enough to quickly scale up or down, resilient organizations have the capacity to adjust. That could mean responding to a crisis by making small modifications to the mission or the technology that supports it. Bigger challenges call for transformative adjustments that some organizations can't easily pull off, such as requests for an agency to execute novel requirements. While no organization can foresee every potential contingency, resilient organizations prepare for the unexpected.

Agencies adjusted to the pandemic at times by shifting existing services to meet demand. Adoption of cloud email by many agencies in the past two years enabled communication among workers to continue as they shifted to home offices. Availability of other communications tools benefited some agencies.

In general, cloud solutions played a major role in supporting agencies during the pandemic's early months, said Suzette Kent, the outgoing Federal CIO. "Scalable, cloud-based, easily configured commercial solutions in so many cases helped us move quickly," she said.

The Ability to Reprocess

Consider the profile of an agency that lacks resilience. It has a process – such as a supply chain workflow – that performs well for sourcing and delivering a product or service critical to the agency's mission. The process relies on legacy technology, but that hasn't been a problem. Without warning, the supply chain workflow becomes disrupted and can no longer function effectively. It can't deliver personal protective equipment or a critical digital resource, such as licenses for VPN, due to a health crisis or some other unanticipated disruption.

The process that had worked well and in alignment with the agency's mission can't handle the new requirement because the process itself is inflexible, supported by outdated, on-premises technology that wasn't engineered for the current environment. The organization and its people, even the budget cycle, are similarly unprepared for a disruption caused by a change in external circumstances. (In this example, financial resources have already been appropriated for other things.) Lacking built-in resilience, the agency must scramble to find ad hoc solutions that will allow it to continue operations.

A resilient agency supported by a modernized enterprise would likely fare better, relying on flexibility, agility and scalability to overcome this supply-chain setback.

Building Blocks

Complexity is the natural antagonist of resilience. It breeds fail points, rigidity, security breaches, and system slowdowns. Reducing complexity is the thread that runs through efforts to bolster resiliency, such as moving data and operations to the cloud; strengthening enterprise IT to improve data management; improving analytics, organizational visibility and cohesion; hardening cybersecurity and expanding mobility.

Data and Operations in the Cloud

Migrating on-premises functions to the cloud is a straightforward way for agencies and their enterprises to become more resilient. Enabling applications such as Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) can deliver operational flexibility and scalability that supports mission continuity in a crisis – or any time circumstances change.

An IaaS is a set of complementary cloud services that allow agencies to deploy applications and services that are accessible from on-premises networks. Using an IaaS such as Oracle Cloud Infrastructure to manage operations in the cloud keeps remote workers connected to data and one another.

Enterprise IT

Compared with modern enterprises, legacy IT is often rigid, inflexible and slow. Moving to cloud and adopting digitally transformative applications improves resilience. Modernizing enterprises makes it possible for agencies to transcend traditional data and operational silos that slow operations and erode efficiency. Agencies find that modernization makes it easier to operate as a holistic enterprise, as opposed to a confederation of disjointed offices that are out of step with one another.

Data Analytics

To further increase resilience, agencies can become more accomplished at leveraging data to make decisions and drive mission outcomes. During times of upheaval and uncertainty, traditional guideposts used for navigation can be unreliable. The ability to use available data to guide operations in real time greatly boosts resilience. Leveraging data at the business end of operations allows agencies to maintain resilience in uncertain environments.

System Visibility

The "fog of war" isn't confined to the battlefield. Lack of visibility into IT systems is a primary contributor to indecision, mistakes and system malfunction in civilian agencies. The modern enterprise embodies a degree of technological complexity that can lead to systemic opacity. It can be difficult at times for system operators to clearly see how well systems are running, where there are slowdowns and even whether there have been intrusions. Clarity into systems contributes to resilience by identifying trouble spots before they become major problems.

Cybersecurity

Cybersecurity is a foundational component of resiliency. Nothing erodes system stability and resiliency faster than security breaches by malicious actors. As enterprises, remote workforces and advanced cloud operations stretch the notion of traditional perimeter security, agencies must stay ahead of would-be intruders seeking to take advantage of larger attack surfaces and the expansion of potential vulnerabilities.

Mobility

The government's response to the pandemic underscored the crucial role of mobility in promoting resilience. Having survived COVID-19's initial impact, agencies must look to the future and prepare for a new way of doing business. As recent months have made clear, mobile devices and applications will be a key component of those preparations. Cloud-based hardware and integrated software deliver mobile solutions that are scalable, flexible and available – anytime, anywhere.

NASA Boldly Explores Telework

During the initial response to the coronavirus pandemic, agencies scrambled to support remote workers while pursuing their missions. NASA, an agency known for succeeding under duress, wasn't exempt. The COVID-19 pandemic imposed significant IT demands on the agency, Seaton said.

Early on, network outages disrupted NASA's remote workers, prompting quickly implemented architectural improvements to resolve those issues. "I like to say that we experienced three years of transformation in the first three months of the pandemic," Seaton said.

To its benefit, NASA had taken steps in recent years to modernize systems and make them more resilient. The agency routinely tested capabilities and trained employees to work remotely and securely. Before the pandemic, some employees regularly worked remotely.

In recent years, NASA invested in modernizing its network, collaboration tools and cybersecurity capabilities, enabling work performed remotely, securely and effectively. By quickly moving most of the workforce to telework status in March, the agency continued operations while limiting employees' exposure to the coronavirus.

The coronavirus has nonetheless provided opportunities for NASA to further improve its systems. "While our VPN availability rate is above 99%, there have been instances of outages that pointed to architectural improvements that we were able to rapidly implement, further strengthening our infrastructure," Seaton said.

The COVID-19 pandemic has provided an opportunity to underscore the importance of IT modernization and the benefits of adopting digital tools, such as recently launched initiatives:

- Development of a mobile/web Contact Tracing & Tracking (CTT) application for entrance temperature screening
- Increase in Virtual Private Network (VPN) capacity
- Launch of Microsoft Teams Mobile Device/Apps
- Enhanced collaborations through audio or video meetings via Instant Meeting, Jabber, Microsoft Teams, WebEx or other NASA conferencing services
- Secure video streaming
- Establishment of a remote process for badge renewals

As most NASA teams moved to remote work in March workers learned to use IT-based collaboration tools like video meetings and collaborative, online content creation.

By the Numbers

NASA has adopted tools to make remote work more personal and interactive:

55,000 users — The capacity of NASA's VPN since a 2019 upgrade

37,000 — The average number of daily users accessing the VPN

> 99% — Network availability

300% — Increased use of Microsoft Teams since March

9,000 — Employees using Teams audio (as of August)

> We are investigating how to effectively bridge on-site and remote employees as we consider the future of work across NASA.
>
> ***- Jeff Seaton, NASA CIO (Acting)***

home-internet connections could largely determine their remote-work experience. "Helping individuals troubleshoot home network performance has been a challenge," Seaton said. "With so many people working remotely, we are reviewing and improving processes for resolving problems and customer outreach."

Seaton predicts that NASA will always have work that is best to do on-site, yet remote work will continue. "We are investigating how to effectively bridge on-site and remote employees as we consider the future of work across NASA," Seaton said.

Despite the early stumbles, NASA's IT systems have performed well, even as the agency tripled the load on some components. As most of the NASA workforce began working remotely, cloud-based email, collaboration and backup tools made it possible for them to work seamlessly and securely.

Looking ahead, effective IT management and proactive cybersecurity will be top priorities at NASA, which for years has deployed IT tools to enable highly-matrixed teams to be mobile and collaborate on complex missions. As NASA transitions more data and capabilities to cloud services, the agency will seek to:

- Train employees to understand benefits and risks in the cloud and their responsibility to protect sensitive data.
- Hold cloud service providers accountable for the security standards established in operating agreements.
- Work with other federal cybersecurity partners, including the Homeland Security Department and the FedRAMP Program office, to ensure NASA is following best business practices, including cybersecurity protocols.

When the next crisis arrives, NASA will be prepared. "We will apply what we have learned to be even better positioned for unforeseen situations we may confront in the future," Seaton said.

NASA remains committed to becoming more secure, effective and resilient. The agency "has risen to the challenge of keeping NASA's missions moving forward during these challenging times," Seaton said. "I have no doubt that they will continue to do so in the future."

Resilient by Design

The Defense Information Systems Agency (DISA) delivers support to the country's warfighters, a critical capability characterized by DISA as its "no-fail" mission. So when the coronavirus disrupted normal operations almost everywhere, DISA was determined to soldier on. Recalling the experience of its experts, on the front lines and behind the scenes, DISA shared with GovLoop insights into its resilience.

GovLoop: The coronavirus pandemic provided an unscheduled stress test of agencies' IT systems. How resilient was DISA?

DISA: As the nation's premier IT combat support agency and part of the Department of Defense's COVID-19 Telework Readiness Task Force, DISA greatly increased telework capacity and other critical capabilities that support the warfighting capacity and lethality of the agency's mission partners. Specifically, DISA enlarged operational capacity by adding new circuits, increasing bandwidth and adding conference call lines.

DISA provisioned circuits that increased capacity by nearly 500 gigabytes. Among the beneficiaries were Northern Command and the Federal Emergency Management Agency's support of the U.S. Navy hospital ships Comfort and Mercy, which operated out of New York City and Los Angeles. DISA supported telework capability by increasing throughput at all of our DISA Internet Access Points. DISA increased Army Virtual Private Network access and reliability by nearly 300% and significantly increased Air Force VPN access.

Leveraging our Joint Regional Security Stack Remote Access VPNs, DISA supported an increase in telework connections for joint partners around the globe by more than 1,000%, from around 8,000 a day to a peak of 122,000 a day.

Has the pandemic exposed opportunities for making government IT systems more resilient?

DISA: In 2019, DISA rolled out its four-year Strategic Plan that supports the National Defense Strategy (increasing lethality, strengthening alliances and reforming business practices) and DoD CIO Digital Modernization Strategy (artificial intelligence; cloud; command, control, and communications; data; and cybersecurity initiatives). Although we had no way of knowing that a global health crisis would happen less than a year later, the strategic plan facilitated DISA's contribution to the whole-of-government response. DISA's acceleration of DoD mobility capabilities enabled government-issued mobile devices to access the Department of Defense Information Network (DoDIN) and information services.

Will the experience of the past six months make resilience a bigger priority?

DISA: The agency's mission connects and protects the warfighter in cyberspace while empowering operations and increasing lethality across every warfighting domain. At DISA, we prepare for a variety of contingencies, making us better able to confront any conflict or crisis.

Probably the biggest challenge for many agencies has been shifting workers from traditional offices to home offices. Is large-scale remote work here to stay?

DISA: The agency is moving into a future that is more mobile, secure and resilient. We've adjusted operations to meet the requirements of this current crisis, and we continue to prepare

for future contingencies. We provided our workforce the tools to perform their missions in this maximum telework environment – an effort that has been incredibly successful.

Did the pandemic stress DISA's capacity to perform its mission?

DISA: Joint Force Headquarters-DoDIN and DISA have risen to the challenge of this crisis every step of the way. People are our greatest asset, and DISA has exponentially expanded DoD's telework capabilities while adjusting to working and collaborating remotely.

Did the challenges of the pandemic strengthen the case for deploying more agile and flexible modern IT systems?

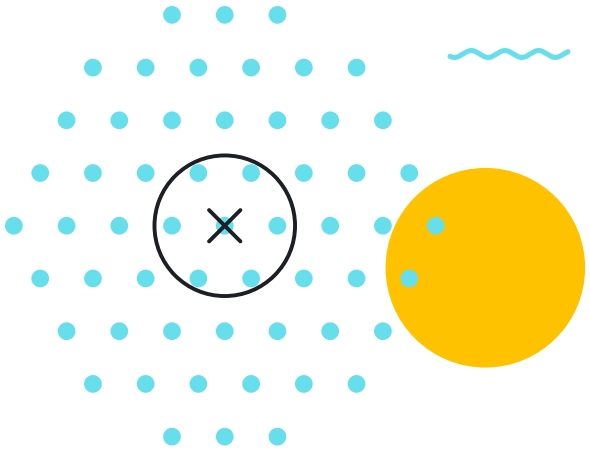
DISA: In addition to greatly expanding telework capacity, DISA also had to support service members, civilians and contractors who were teleworking in many cases without government-furnished equipment. They needed audio and video conferencing, chat and other collaboration capabilities, which we quickly availed. This led to adopting Microsoft's Teams solution, the Commercial Virtual Remote Environment or CVR, which has been widely adopted across the department, enabling them to work on personal devices.

Do you foresee federal agencies, including DISA, embracing more mobile solutions supported by the cloud?

DISA: For years, DISA has been moving toward a more mobile-capable workforce that can access data anywhere and at any time. We want many of these force-strengthening changes to be enduring.

Having weathered the coronavirus storm, will agencies be more prepared for the next unexpected crisis?

DISA: The agency continues to focus on making our workforce, networks and data more mobile, secure and resilient. DISA always prepares for a variety of contingencies, and those preparations will make us better able to handle any conflict or crisis we face in the future.



Resilience to the Fore

An interview with David Knox, Group Vice President for Public Sector Software Sales, Oracle

Enterprise complexity is not just about complex systems. It's also about the diverse array of technologies and technological eras that coexist in some IT ecosystems. Those complex systems tend to function well when their disparate components are in a state of equilibrium. Events that alter demands on the system or any of its components, however, can disrupt equilibrium, essentially knocking components out of their functional orbits and alignments within the system. Invariably, performance suffers.

"Systems built many years ago are still functioning, but their architectures are from a different era," Knox said. "Security may be rather rudimentary compared to today's standards. That creates complexity."

Multigenerational systems composed of dissimilar technologies aren't just complex, they're inherently unstable. Such environments are nonlinear and marked by intricate tendencies. "One system feeds another two different systems and then something else comes in and aggregates and summarizes something from something else. It's quite a hairball of complexity," Knox said. "Resiliency is tricky."

Indeed, deploying capabilities for strengthening system resiliency, such as backups and recoveries, can be challenging in a complex environment. The architecture of some technologies will not support functionality considered routine in a modern system. Weekly backups of data, with incrementals done nightly, may not be possible. Creating service level agreements or recovery time objectives can be difficult as well.

Identify Disruption

To understand when resiliency is inadequate, identify and understand the metrics of disruption. Consider the metrics of call center productivity and volume. Managers could seek to identify data thresholds that serve as triggers of disruption. "Go through the process of gaining situational awareness," Knox said. "From there you can put together an improvement plan. Start simple. Take a crawl-walk-run approach."

A key component of such a plan will be rigorous, regular maintenance. "Successful agencies have actively practiced good IT hygiene," Knox said. "They've been diligent about keeping systems and processes updated to the latest technologies and best practices."

The pandemic exposed the challenges of complexity, including the difficulty of scaling complex systems. Resilience requires agility – the ability to make slight, sometimes frequent, alterations to technology, processes or organizational goals – while staying within budget and staying true to agencies' missions.

"Some systems broke because suddenly they were under duress at a level that was orders of magnitude higher than ever thought possible," Knox said.

Next Steps

Having survived the initial disruption of the pandemic, take time to identify specific lessons learned, which will differ slightly between agencies. Develop a strategy to mitigate future situations that could impact the mission. Create an actionable roadmap that can be quickly operationalized.

With budgets likely to be tight in the near term, leverage existing investments smartly. If you have an on-premises license with Oracle, for example, you can transfer some older investments. "Repurpose dollars already spent to augment what you have with cloud capability," Knox said. "In the cloud world, universal credits give agencies complete flexibility on what they can do in the future."

How Can Oracle and Affigent Help?

Affigent and Oracle help agencies develop best practices for promoting resilience. Oracle's autonomous services mitigate demands on human workers and allow them to work on higher-level challenges. Employees can work from home because technology is smart enough to administrate itself. Agencies rely on Oracle and Affigent's expertise for scaling up, scaling out and understanding how to build a resilient environment. Luck favors the prepared.

Affigent
AN AKIMA COMPANY

ORACLE Platinum Partner

Accelerate Your Move to the Cloud

Affigent, an Akima Company, provides streamlined access to Oracle's full suite of hardware and services through GSA Schedule 70.

The benefits of purchasing through Affigent on GSA include:

- A shortened, streamlined procurement process
- Agility to meet customers' needs with millions of products and services
- Volume discount pricing
- Multi-year agreements

Visit affigent.com/products/oracle to learn more

Conclusion

The coronavirus and its continuing impact on America's institutions has given federal agencies good reason to re-evaluate enterprise modernization plans and the timetable for attaining them. Moreover, the crisis has provided a roadmap for advancing IT modernization and bolstering resiliency. Among the lessons learned:

Resiliency Begins With People

Agencies throughout the government marshaled resources to survive the black swan event known as COVID-19. By and large, employees performed admirably. Some 2 million workers migrated en masse from government offices to home offices. Through long hours and heroic efforts, workers made it possible for the government to stay open at a time when millions of Americans desperately needed government services and emergency relief. When it mattered most, government workers were resilient in ways that exceeded the capabilities of digital solutions. According to the Government Accountability Office (GAO), federal employees' productivity increased after they began teleworking.

Less Legacy, More Agility

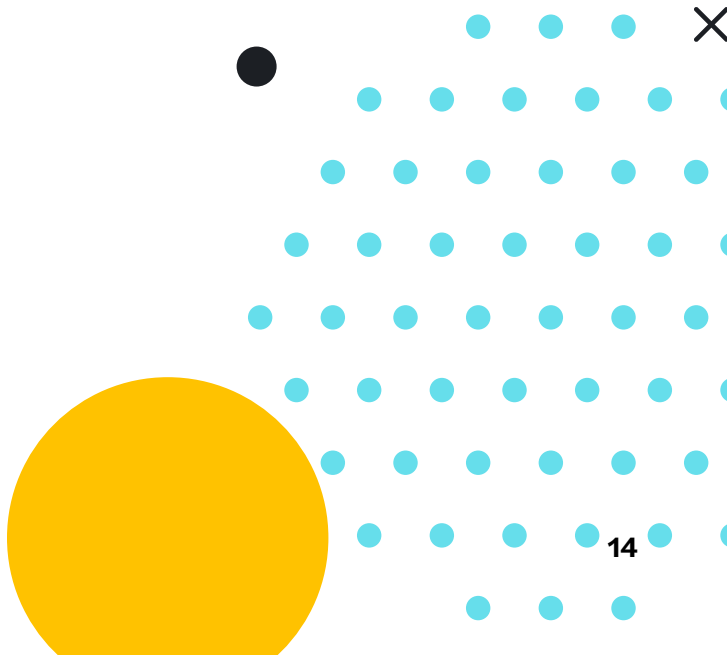
The crisis spotlighted the need to replace outdated systems incapable of easily responding to shifting circumstances. During the pandemic's early phase, outdated technologies groaned, sagged and threatened to break beneath the dual challenges: standing up a massive remote workforce while also meeting sharply increased demand for some government services. If not for the allocation of billions in emergency funds and timely policy changes, some agencies would have been overwhelmed.

Accelerate Modernization

The pandemic proved the value of digital modernization. Agencies prevailed, in large part, by accelerating modernization initiatives already underway, such as expanding bandwidth and taking advantage of cloud-based applications, from teleconferencing to telemedicine. Absent a massive shift to cloud resources, the VA would have been unable to adequately support at-home workers or deliver health care to millions of veterans. Some of the emergency actions taken to avert a bigger crisis had been planned for some time but lacked funding until Congress provided emergency allocations.

Now, government leaders are asking themselves how they can put modernization – and resilience – on a faster track. The experience of COVID-19 has taken the sting out of concerns that impeded modernization in the past, mostly fear – of failure, the unknown, choosing the wrong solution, and funding.

If agencies can rise to the occasion and embrace digital transformation in a crisis, can they persevere and carry on when the crisis has passed?



Thank you to Affigent and Oracle for their support of this valuable resource for public sector professionals.

To learn more, please visit www.oracle.com

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.

www.govloop.com | @GovLoop