



RESILIENT

KEEPING YOUR WITS—WORKFORCE, INNOVATION,
TECHNOLOGY, SECURITY—ABOUT YOU

JANUARY 2021



PARTNERSHIP FOR PUBLIC SERVICE



The Partnership for Public Service is a nonpartisan, nonprofit organization that works to revitalize the federal government by inspiring a new generation to serve and by transforming the way government works. The Partnership teams up with federal agencies and other stakeholders to make our government more effective and efficient. We pursue this goal by:

- Providing assistance to federal agencies to improve their management and operations, and to strengthen their leadership capacity.
- Conducting outreach to college campuses and job seekers to promote public service.
- Identifying and celebrating government's successes so they can be replicated across government.
- Advocating for needed legislative and regulatory reforms to strengthen the civil service.
- Generating research on, and effective responses to, the workforce challenges facing our federal government.
- Enhancing public understanding of the valuable work civil servants perform.

The voice of tomorrow's government today, **MeriTalk** is a public-private partnership focused on improving the outcomes of government IT. Our award-winning editorial team and world-class events and research staff produces unmatched news, analysis and insight. The goal: more efficient, responsive and citizen-centric government. MeriTalk connects with an audience of 160,000 federal community contacts. For more information, visit www.MeriTalk.com or follow us on Twitter, @MeriTalk. MeriTalk is a 300Brand organization.

ACT-IAC is a nonprofit educational organization established to improve government through the effective and innovative application of technology. ACT-IAC provides an objective, trusted, vendor-neutral, non-partisan and ethical forum where government and industry executives can communicate, collaborate and learn. ACT-IAC provides a public-private partnership in the government technology community and has been called "an example of how government and industry can work together."



INTRODUCTION

The COVID-19 pandemic will be remembered as a defining moment in the history of the federal government. More so than any crisis in a generation, it highlighted the extent to which the resilience of the United States relies on the resilience of its government. It also presented an opportunity for federal leaders to rethink and reset how their agencies deliver their missions. Returning to the pre-pandemic status quo can no longer be the goal.

In this environment, the American Council for Technology–Industry Advisory Council, MeriTalk and the Partnership for Public Service, with support from our corporate partners, saw an opportunity to help government chart a path forward. We commissioned a survey of 300 federal leaders that identified vital lessons learned over the course of the pandemic, and we held roundtable discussions to explore in depth four issues that are essential to government resiliency: workforce, innovation, technology and security, or WITS.

This report encapsulates our findings, and it provides detailed recommendations for future operations, service delivery and policymaking that should become priorities in 2021 for leaders within the Biden administration and Congress. They must keep their WITS about them as they seek to transform government and improve its resilience. With nearly nine out of 10 respondents in our survey affirming that America’s resilience depends on the resilience of its government, it’s time to act decisively.

We found that the majority of agencies navigated the pandemic effectively, continuing to deliver on their missions amid the uncertainty. The Internal Revenue Service, for example, distributed billions of dollars in stimulus payments to millions of individuals in only two months. The Department of Veterans Affairs handled an almost fifteenfold increase in telehealth appointments for veterans’ physical and mental health services. These agencies—and many others—were willing to experiment and able to adapt to unprecedented demand for government services.

Other agencies stumbled. Federal public health agencies, for example, struggled to collect and share accurate healthcare data with states, local governments and private partners. For some agencies, the coronavirus highlighted the challenges already posed by government struggles with antiquated technologies, retention of high performers and cumbersome rules for budgeting and procurement.

During our roundtable discussions, federal leaders told us that for government to become more resilient, it must build:

An agile workforce

prepared to face changing circumstances, from global crises to evolving customer expectations.

A culture of innovation

that encourages staffs to constantly seek new and better ways of doing business.

A modern technology infrastructure

that helps employees do their jobs more effectively.

A cutting-edge cybersecurity posture

that keeps technology tools, data and information secure and private.

“Now is the time for us to be thinking about how to reinvent government. How do we use technology to make what we used to do easier and better? How do we create workplaces that drive creativity and engagement? We have a chance to create a new future and not just dust off the old future. Think about what you want your agency to be like, then brainstorm with your teams how to do it.”

—Juliana Vida, chief technical advisor, public sector, Splunk

Methodology

In August and September of 2020, ACT-IAC, MeriTalk and the Partnership for Public Service surveyed 300 federal information technology executives and mission owners, including human capital managers, to understand their priorities, aspirations and pain points around federal resiliency. The leaders surveyed were at the program manager level and above, working in civilian, defense and intelligence agencies in jobs relating to technology, security, data, and business and program management. The survey focused on the areas of workforce, innovation, technology and security. The survey had a margin of error of $\pm 5.62\%$ at the 95% confidence level.

The results of the survey served as a foundation for four discussions we hosted in October and November 2020 with more than 50 federal leaders and private sector experts on workforce, innovation, technology and security. Discussants reflected on survey results, their own organization's experience in managing the COVID-19 pandemic and lessons learned for improving government's resilience to future crises.

Leaders also said agencies should view workforce, innovation, technology and security as interconnected, rather than as separate issues. Conversations underscored the degree to which these areas are interdependent, and how shortcomings in one might leave government vulnerable in another. For example, underinvesting in the workforce's technology and cybersecurity know-how might leave agencies unprepared for cyber threats, while falling behind in innovation might keep them from acquiring and using the newest technology systems. Leaders also stressed the importance of putting customers first, to ensure seamless and satisfying delivery of government services.

Eighty-five percent of federal leaders surveyed agreed that the COVID-19 pandemic presents a watershed moment for modernizing the federal government. To capitalize on this transformative opportunity, federal leaders recommended that government:

Cultivate a flexible workplace culture.

Empower employees to innovate through praise and policy.

Adopt cloud computing, expand access to technologies and improve the customer experience.

Emphasize the importance of cybersecurity and invest in modern cybersecurity methods and tools.

The COVID-19 pandemic transformed the federal government, upending operations and amplifying the urgent need for resilience during crises. It forced government leaders to think outside traditional boundaries of service delivery and find new ways to collaborate with state and local governments, private companies and international partners. Within this report, we outline top issues and key considerations for leaders in the Biden administration and Congress in workforce, innovation, technology and security; show how several agencies successfully adapted to serving people during the COVID-19 pandemic and outline the challenges they overcame; and detail new approaches for agencies as they work to improve their resiliency.

WORKFORCE

Cultivate a flexible workplace culture

The workforce is an organization's most important asset. Employees play a critical role as organizations manage change during and after crises occur. Therefore, recruiting, hiring, retaining and training a skilled and experienced workforce is central to resilience.

The findings from ACT-IAC, MeriTalk and the Partnership's survey underscored the importance of the workforce. When asked about what a resilient federal government looks like, one in two respondents associated it with an agile workforce—one that can adapt to changing customer needs and external circumstances. More respondents linked resilience to an agile workforce than to cutting-edge cybersecurity, modern technologies or continual innovation, the other issue areas featured in this report.

Federal employees seemed to be satisfied with remote agency operations. In one agency's survey on remote work, 85% of respondents reported feeling supported by their managers, and 80% felt engaged with their peers and colleagues.

The workforce's commitment to public service and agency missions could be behind its resilience. In our discussions, federal leaders with a background in psychology highlighted that a sense of purpose—an emotional connection to serving the public and delivering on the mission—could account partly for why federal employees were able to adapt successfully to changing circumstances and a new way of doing business. Scientific studies have indeed shown that having a strong sense of purpose improves an individual's resilience in facing adverse situations.^{7,8}

Despite federal employees' resilience in facing the COVID-19 pandemic, long-standing workforce challenges remain to be addressed if agencies are to become more resilient in the future. Most acutely, 85% of survey respondents believed their agency has workforce skills gaps that adversely affect resilience. These gaps were often present before the coronavirus hit, but the pandemic made them more obvious. Federal leaders in our discussions agreed a shortage of employees with the skills central to navigating a changing world—skills related to emerging technologies, data science, change management and business process reengineering—hampers government's ability to deliver on the mission because of ever-evolving obstacles.

Our research uncovered several issues that might contribute to the skills gaps. The top five challenges survey respondents highlighted were: the lengthy federal hiring process, uncompetitive compensation compared to the private sector, not enough qualified candidates applying to fill open roles, a lack of understanding of future skills needed, and a dearth of relevant training programs. In our discussions, federal leaders noted the fierce competition for talent among agencies and between the public and private sectors in cities where their agencies are located, especially in the Washington, D.C., metropolitan area.

Recommendations for the workforce

During our discussions, federal leaders focused mostly on creating a flexible workplace for employees. Participants said the pandemic has shattered negative notions around telework, proving that moving the mission forward with remote workers is a viable option that does not impinge on employee productivity. Several agencies that



One in two survey respondents associated resilience with an agile workforce.

An essential feature of an agile workforce is a workplace where employees have flexibility in when and where they get the job done, including the ability to work outside the office. Agencies shifted to telework on a large scale during the pandemic, with more employees working remotely at more agencies than ever before. For example, some 95% of Department of Labor employees worked remotely through most of 2020. Even agencies with restrictive telework policies changed their posture and allowed for expanded remote working, enabling employees to continue delivering on the mission, federal leaders said. "The pandemic showed that we can get the job done even remotely," said Gundeep Ahluwalia, chief information officer at the Department of Labor.

"There is no one-size-fits-all approach to remote work. Recognizing what's feasible to successfully execute the mission, federal agencies should accommodate reasonable combinations of in-home or at-office work environments that support employee needs and preferences."

— Margaret Cunningham, principal research scientist for human behavior, Forcepoint X-Labs

Several tried-and-tested strategies were discussed as options employees could consider for reducing the risk of burnout and attrition. They could create a dedicated workspace at home to improve the separation between work and rest. They should take short breaks during the workday or use their vacation days. Employees also could participate in meetings while walking outdoors.

Federal leaders also should encourage informal meetings and brown-bag lunches that enable employees to socialize. Finally, leaders should watch out for warning signs that might indicate an employee is struggling, such as if someone is offline for prolonged periods during the workday or is not responding to emails or calls from colleagues or supervisors.

1 Stacey M. Schaefer, "Purpose in Life Predicts Better Emotional Recovery from Negative Stimuli, PLUS ONE 8(11), 2013. Retrieved from <https://bit.ly/35GwdoY>

2 Sherry Hamby et al., "Poly-victimization, Trauma, and Resilience: Exploring Strengths That Promote Thriving After Adversity," *Journal of Trauma and Dissociation* 21(3), January 2020. Retrieved from <https://bit.ly/3kG2roH>



The **Department of the Treasury** is viewing the current situation as an opportunity to rethink its recruitment strategies and to access talent outside its Washington, D.C., headquarters. One possibility is hiring and building smaller employee teams in several locations across the country. This would enable the agency to recruit talent across the country while also giving these employees the option of working and collaborating both virtually and in a more traditional office environment.

Top recommendations

Federal agencies should:

- Work with individual employees to determine the best option for how, when and where they get their work done, based on personal work styles and circumstances.
- Use workplace flexibilities to tap into new pools of talent, such as people who live farther than commuting distance from agency headquarters.
- Encourage collaboration between HR and IT staff. Remote work and collaboration depend on technology, which means IT teams will continue to play a critical role in building resilient agencies that support their employees. The collaboration between HR and IT should also extend to training employees to use new technologies and creating agency cultures that embrace the use of these tools.

had restrictive telework policies up until early 2020 shifted their stances during the pandemic and are now seeking to allow more remote work in the future.

Not all employees will want to continue working remotely when a return to the office becomes an option. While some employees are more productive working from home, others have found they are more productive when collaborating in person, or that they do not have the technology to support remote work in the long run.

Agencies need to work with individual employees to determine the best option for how, when and from where those individuals get their work done, based on personal work styles and circumstances. Managing and monitoring performance also should be tailored to fit the unique needs of employees working remotely and those who return to an office to work in person. “Recognizing there is no one-size-fits-all approach to remote work, federal agencies should respect individual preferences and allow employees to work where they want and how they want,” said Margaret Cunningham, principal research scientist for human behavior at Forcepoint X-Labs. “The future of work will be flexible,” added Department of Labor Chief Information Officer Gundeep Ahluwalia, with some employees working remotely almost all the time and others working from agency offices.

Our survey findings reinforced the need for a more flexible workplace to support employees, with 45% of respondents stating they believed creating a work environment with flexible hours and the option of remote work is among the most important workforce-related changes agencies should make to improve government’s resilience.

However, the pandemic also highlighted the potential adverse impact of remote work on the work-life balance of many employees. Many leaders said they became concerned about employee burnout, with home offices blurring the boundary between work and home lives. Federal leaders warned that several agencies attributed some increases in productivity to remote employees working longer hours—which could lead to employee burnout, which in turn could cause higher staff turnover and attrition.

Workplace flexibilities could help government address skills shortages and create an agile and mobile workforce. With remote work likely to remain prevalent in federal agencies, leaders could tap into new pools of talent consisting of people who live farther than commuting distance from agency headquarters. Agencies could reach people who did not consider working for a federal agency because they did not want to move to Washington, D.C. Additionally, the ability to recruit talent nationwide would lessen the difficulty agencies face now of having to compete with the public, private and nonprofit sectors for D.C.-area talent.

To maintain an agile workforce and a flexible workplace, HR teams must work “hand-in-glove” with information technology staff, said Jennifer Ackerman, deputy chief human capital officer at the Department of Interior. Others agreed. Remote work and collaboration depend on technology, which means IT teams will continue to play a critical role in building resilient agencies that support their employees. HR and IT staff should work together to find new tools, from videoconferencing to virtual collaboration platforms to cloud computing, that support agency staffs regardless of where and how they work. The collaboration between HR and IT should also extend to training employees to use new technologies and creating agency cultures that embrace the use of such tools, federal leaders said.

INNOVATION

Empower employees through praise and policy

The federal leaders with whom we spoke said implementing new approaches to tackle old problems is a pathway to building a resilient government. Organizations that encourage their employees to innovate on the job are more resilient than those that do not. Their commitment to finding new ways of doing business is good preparation for undertaking the transformation needed to respond to external shocks. On the other hand, risk-averse organizations that do not encourage innovation are less amenable to change and thus less resilient in times of crisis.

Our survey findings also underscored the importance of innovation. When asked what the federal government should do to improve resilience, 49% of respondents said it should immediately focus on encouraging continual innovation. Only 10% of respondents believed innovation need not become a priority in the short term.

During our discussions that built on the survey findings, federal leaders said that many innovations were born of necessity. Government agencies had no choice but to adapt to changes if they were to continue delivering services to the public, according to Sanjay Gupta, chief technology officer at the Small Business Administration. “Necessity is the mother of innovation, to use a slightly modified version of the metaphor,” Gupta said.

Because the COVID-19 pandemic showed that government has the capacity to innovate, participants agreed agencies should maintain the culture of innovation beyond the current crisis. “It would be a shame if we lost all the capabilities we have demonstrated. Instead, we must continue building on them,” Gupta added.

Recommendations for innovation

When asked about the most important changes needed to support innovation, a third or more of survey respondents said leaders should empower their employees to be creative, remove internal agency barriers to effectiveness, and increase support and communication for making innovation a priority.

Policy also plays an important role in supporting or hindering innovation, federal leaders said. While policies are important guardrails that prevent misuse of taxpayer funds and guide agencies in mission delivery, agencies should not be “misguided” or “inhibited” by perceived policies, the leaders said.

Federal leaders said assessing an agency’s appetite for risk also can foster innovation by helping employees balance risk and reward in their pursuit of changes and efficiencies for improving mission outcomes. By assessing risk appetite, an agency signals the degree to which it is willing to tolerate risk in doing business and what types of risks are accepted, even encouraged. The leaders said employees should first identify the types of risk their agency faces in achieving its objectives, whether it is security, financial, reputational or some other risk, and what impact these risks have on the mission. They should then determine how much tolerance the agency has for each category of risk.

To support innovation, leaders encouraged the use of ideation platforms—online tools that enable users to work with others to develop, test and refine ideas for solving problems. Having access to such platforms empowers employees to come up with new ways of doing business and enables leaders to tap into the collective knowledge and expertise of their staffs rather than only seek solutions from outside the agency. “Ideation platforms connect employees working across



In March 2020, the **Small Business Administration** was able, in six hours, to set up a new web portal as a stopgap measure for applying for disaster loans while a new web portal was being developed. This stopgap solution received about 500,000 files in the first 100 hours after going live. Around the same time, the agency deployed, within a few days, a new cloud-based case management tool to organize incoming emails from its small business customers, creating the capacity to scale up customer support, and over a 40-day period a million cases were created in this case management tool.

The **Department of Veterans Affairs** managed a surge of an additional 100,000 in the number of employees who worked remotely in the first few months of the pandemic, partly by turning to cloud computing.

The **Veterans Health Administration** overcame well-known federal hiring challenges to onboard more than 55,000 new employees between March and October 2020.⁷

From a policy standpoint, some agencies did not have formal policies or capabilities for remote work. COVID-19 has taught those in government that they can move faster than they realized. The **National Geospatial-Intelligence Agency** had policies limiting remote work due to mission and security concerns but found that secure remote work was possible. Within two weeks in spring 2020, the agency was able to quickly deploy virtual desktop capabilities through which tens of thousands of employees can access agency applications from their personal devices.

3 Partnership for Public Service and Democracy Fund, “Rapid Reinforcements: Strategies for surge hiring,” October 2020, 13. Available at <https://bit.ly/35Zpiq2>

In 2017, **SBA** began moving its infrastructure from agency-owned data centers to the cloud but ran into roadblocks when trying to ensure its new cloud infrastructure complied with federal cybersecurity policies, such as the Trusted Internet Connections. In early 2018, in collaboration with the Office of Management and Budget, the Department of Homeland Security and the General Services Administration, SBA conducted a 90-day TIC modernization pilot which demonstrated that the agency met the overall goals and intent of the TIC policy in its cloud environment. This pilot program informed OMB's update to the TIC federal cybersecurity policy and also enabled overall cloud adoption across the federal landscape.

The **U.S. Agency for International Development** assessed its risk appetite and published a statement in 2018, which helped staff and partners around the world better understand how to navigate risk, including both the threat and opportunities embodied in risk navigation. The assessment helped USAID determine its level of risk appetite in different categories. For example, the agency identified that it has a higher tolerance for programmatic risks, recognizing that smart risk-taking is necessary for achieving the agency's long-term objectives, and to pursue new, more effective and innovative approaches and technologies. This also recognized that risk was already a fundamental element that USAID programs navigated every day in delivering critical support to insecure, complex and challenging environments. Conversely, the agency said its legal risk appetite is low, due to its need to protect against unlawful actions that could harm the public.⁴

"Innovation labs are very successful at fostering cutting-edge ideas. They encourage small teams of forward-looking talent to come together to tackle mission-critical challenges, try new technologies and adopt innovative business practices, making operations more effective and efficient."

— Cindy Hewitt, senior manager, AWS

⁴ U.S. Agency for International Development, "U.S. Agency for International Development Risk Appetite Statement – June 2018," 8, 14. Retrieved from <https://bit.ly/2G6kjuJ>

the country and allow them to brainstorm with colleagues at any time from any location. They are so powerful. They are one of the best tools in any innovation toolkit to focus on customers first with solutions," said Daniel McCoy, chief innovation officer at the Transportation Security Administration.

During the pandemic, the Transportation Security Administration monitored its ideation platform to inform how it protects employees from the coronavirus. Through the platform, agency leaders set out to gauge staff satisfaction with personal protective equipment to keep employees safe. The feedback helped TSA to recognize that protective equipment preferences existed between airports and roles. Input from employees in the field will help shape future requirements for PPE, shielding and technology, all adjusted to keep both passengers and officers safe.

Survey respondents also highlighted the need for innovation in collaborating remotely, with 39% saying that is where agencies should focus their efforts. Federal leaders agreed that videoconferencing technologies that allow for effective remote collaboration—and that the pandemic made commonplace—should remain integral to agencies' functioning once they adjust to work after the pandemic. "Tools like VA's own Video Connect solution, Zoom, Teams and Webex are now like a No. 2 pencil. We are using them all the time, they are so natural for us," said Jack Galvin, associate deputy assistant secretary of the Office of Information and Technology at the Department of Veterans Affairs.

Top recommendations

Federal agencies should:

- Use proven methods for encouraging innovation: back employees and teams that experiment with creative projects, position staff to identify and implement new ideas, reward employees who identify better ways to do their work, actively and frequently review and revise outdated processes, and implement processes and technologies that improve performance.
- Assess the appetite for risk, which can foster innovation by helping employees balance risk and reward as they pursue changes and efficiencies to improve mission outcomes.
- Encourage the use of ideation platforms—online tools that enable users to collaborate to develop, test and refine ideas that solve problems.

TECHNOLOGY

Adopt cloud, expand access and improve the customer experience

Technology underpins the business of government. Computers enable agencies to store, retrieve, transmit and manipulate data and information, communications tools to interact with customers, and emerging technologies to explore new ways to achieve the mission.

But the COVID-19 pandemic made technology even more important to agencies. In the past, technology enabled agencies to seek efficiencies and complemented in-person and paper-based services. During the pandemic, it became essential for agencies to keep functioning. Indeed, 42% of respondents in our survey said that at least half the IT they use for work needs to be updated or replaced to reflect this reality.

Federal employees were largely satisfied with their agencies' focus on technology to support them and the mission, with 82% of respondents in the survey "very" or "somewhat" satisfied; only 17% were "not very" or "not at all" satisfied. And 82% of respondents said their agencies' IT teams were "very" or "somewhat" effective in helping staff shift to remote work.

The survey also identified steps respondents wish their agencies had taken to prepare for the COVID-19 pandemic. Several respondents said their agencies should have better trained their employees to use digital tools for collaboration, prepared more robust communications networks to handle remote connections, and transferred more data to the cloud so it is available to all employees working from any place and at any time.

Many agencies have long struggled with IT challenges. In fiscal 2019, the federal government planned to spend about 80% of its more than \$90 billion IT budget on maintaining information systems, including legacy IT, according to a 2019 Government Accountability Office report.⁵ GAO also found that several systems critical to agency functioning were more than four decades old, posing high cybersecurity risks for several Cabinet departments.

Recommendations for technology

To improve their resilience further, agencies must make several changes to address longstanding technology challenges. Survey respondents identified the five top changes agencies should pursue: expanding remote access to technologies, increasing technologies' reliability, increasing cybersecurity, reducing the reliance on legacy technologies and increasing computer processing speeds. In our discussions with federal leaders, the need to expand remote access to technologies and modernize legacy IT rose to the top.

With the pandemic reshaping government's approach to remote work—shattering notions of its negative impact on productivity and proving the feasibility of remote work in the long run—federal leaders agreed that agencies should improve their technology capabilities to support remote workers. "Agencies should embrace remote access to services and information on a permanent basis," said Joseph Klimavicz, managing director at KPMG and former chief information officer at the Department of Justice.

Several steps are necessary to support long-term remote work. Agencies should create plans and policies that allow employees to use their own devices, such as personal desktops and laptops, to do their work and access agency networks.



In response to the pandemic, many agencies expanded their technology use and launched entirely new technology initiatives. The **Department of Veterans Affairs** acquired and shipped 225,000 laptops to accommodate remote workers in 2020. The Department of State created software applications to organize its efforts to bring more than 100,000 Americans back to the U.S. at the beginning of the pandemic.⁶ And the **Department of Energy and Office of Science and Technology Policy**, alongside private companies, put the supercomputing capacity of national laboratories behind the research into COVID-19.

The **Small Business Administration** supported remote workers by giving them access to cloud-based technology tools, such as the Microsoft Office suite of applications, from any device. The agency put safeguards in place to keep systems secure: It enabled multifactor authentication to verify a user's identity and right to access a system and disabled the option to download documents to the personal device's hard drive. It also instituted conditional access policies, under which the agency checked if the users were authorized to access a file or system based on, for example, their IP address or location.

"When new systems are launched, there is a tendency not to continue to modernize them. They keep those systems running, making patches as needed, but are not taking on a roadmap to modernization and outlining what is next for those systems. But it should not be a one-and-done approach. With continuous modernization, you should modernize and improve parts of those systems as they age, making small changes with a broader plan in mind. Then, at the end of a particular system's life cycle, you are not faced with a massive project to implement a new system and modernize everything at once."

—Christopher Haas, strategic business executive, Google

5 Government Accountability Office, "Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems," GAO-19-471, June 2019, i. Retrieved from <https://bit.ly/34eO8lF> (PDF)

6 Jory Heckman, "State Department 'reimagine taskforce' collecting IT lessons learned during COVID-19," Federal News Network, Nov. 13, 2020. Retrieved from <https://bit.ly/3nvoeRP>

Modernizing legacy systems and moving them to the cloud will become even more important with flexible work arrangements expected to remain prevalent. Indeed, one in two survey respondents said the cloud should be among the most important technologies in their agencies. “Cloud is the foundation agencies must build on,” federal leaders agreed.

Cloud computing, which offers information networks that can be accessed anywhere at any time, is also flexible and scalable, enabling agencies to adapt to sudden increases or decreases in network use. That happened almost overnight when tens of thousands of employees had to start working remotely in the wake of the spread of the COVID-19 pandemic.

The modernization of legacy systems and their migration to the cloud is a continuous journey. Even after legacy systems are replaced, agencies need to continually update those systems. “When new systems are launched, there is a tendency not to continue to modernize them. But it should not be a one-and-done approach,” said Christopher Haas, strategic business executive at Google. Continued improvements are necessary to update systems when mission delivery needs change, such as when a new law alters who is eligible to receive a service, or when new security or privacy rules are put in place.

Delayed IT modernization makes technology transformation more difficult down the line. Agencies often add new public-facing websites or software applications on top of legacy technologies, increasing the complexity of the interconnected systems. Systems patchworked this way add complexity, and agencies need more technical know-how, time and money to upgrade them. One leader called this accumulation of technical complexity an agency’s “technical debt,” which becomes harder to pay off with time.

Agencies should keep their customers in mind as they turn to new technologies. Members of the public have raised expectations for a seamless and satisfying customer experience, based on expectations set by the private sector. When interacting with government agencies, people increasingly want to access services from any device, whether a laptop, tablet or smartphone. Agencies should ensure their websites and online applications for services meet this demand, federal leaders said.

Customers also increasingly prefer self-service capabilities, such as being able to check when their service or benefit might be delivered, without calling a call center or visiting an office in person. Therefore, agencies should create websites that enable their customers to easily check the status of an application or benefit.

Federal leaders agreed that budget constraints limit their ability to modernize legacy systems. Most legacy IT cannot be upgraded within government’s traditional 12-month budget cycle. Agencies need multiyear funding certainty to pull the plug on old systems. Potential solutions include two funding mechanisms that provide funding

stability in an era when Congress passes repeated continuing resolutions, an activity that exacerbates budget uncertainty and prevents agencies from planning for the long run:

- The Technology Modernization Fund is one potential solution. Agencies can tap the fund to pay for long-term modernization efforts.
- IT working capital funds, authorized under the same Modernizing Government Technology Act that created the Technology Modernization Fund. Through working capital funds, agencies can set aside unspent IT dollars and use them later for technology modernization projects.

Federal leaders also discussed the importance of sharing the data and information in their IT systems. Building on the Federal Data Strategy and its 2020 action plan, which establish best practices for using data and outline initial steps for implementing the best practices across government, agencies should continue to find ways to share data between programs, offices and agencies.

For data-sharing to be feasible among all agencies, government must establish data standards, from shared file types and naming conventions to a common way of identifying customers. Once data standards are established, agencies could purchase new shared technologies that can seamlessly access, read and share data from any agency. Shared technology tools could improve collaboration and reduce duplication among agencies, leaders agreed.

Top recommendations

Federal agencies should:

- Modernize legacy systems and move them to the cloud, while recognizing that this is a continuous process, not a one-time move.
- Seek multiyear funding opportunities to support technology modernization, such as requesting funds through the Technology Modernization Fund or setting up IT working capital funds.
- Establish data standards, from shared file types and naming conventions to a common way of identifying customers, as a way to encourage data sharing among agencies and offices. Once data standards are established, agencies could purchase new shared technologies that can seamlessly access, read and share data from any agency.

SECURITY

Emphasize its importance and invest in the future

Cybersecurity, a critical element of any organization's resilience, has been indispensable to the federal government's response to the COVID-19 pandemic. Early in the pandemic, security considerations moved to the forefront as more employees than ever before worked and accessed agency information networks remotely and used digital tools to continue operations and service delivery.

Our research showed government was largely up to the security challenge: Federal leaders thought highly of government's efforts to keep them and their data safe from unauthorized users. In our survey, 44% of respondents said they were "very satisfied" and 45% "satisfied" with their agency's focus on security to support government resilience. Indeed, the federal executives in our survey were most satisfied with their agencies' focus on security compared with their agency's focus on the workforce, innovation or technology.

Federal leaders discussed several potential reasons for the satisfaction with agency security efforts.

Agencies had a robust cybersecurity foundation to rely on during the pandemic thanks to previous concerted efforts to improve government's cyber posture. Since the 2000s, the White House and Congress have continued to emphasize the importance of cybersecurity in moving government's mission forward, launching new cybersecurity initiatives and expanding existing ones.

Among the cybersecurity initiatives, federal leaders in our discussions highlighted the importance of the:

- Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act of 2014, both of which require agencies to develop and implement plans to protect their information systems.
- Trusted Internet Connection initiative, started in 2007, which sets security policies for government's internet capability and use.
- General Services Administration's Continuous Diagnostics and Mitigation program, launched in 2013, which gives agencies the technology capabilities needed to strengthen their cybersecurity.

Collaboration also played a role in securing government business during the pandemic. The Department of Labor, which works extensively with state and local governments to provide services and benefits to the public, attributed its success partly to close collaboration with private information technology and security firms. Gundeep Ahluwalia, the department's chief information officer, said that when the pandemic's economic toll became obvious, several private companies offered to help rapidly bolster, upgrade and secure systems the federal, state and local agencies relied on to manage the unprecedented demand for services, a testament to how the cybersecurity community came together when facing a common threat.

Recommendations for security

The federal leaders with whom our organizations spoke said cybersecurity will remain critical for building government's resilience to future crises. Ahluwalia described the efforts needed as "a marathon, not a sprint," necessitating a "sustained focus over many years." Survey findings echoed the sentiment about cybersecurity expressed in our discussions: 45% of respondents said a resilient federal government requires a focus on cutting-edge cybersecurity.

Recommendations related to hiring cybersecurity talent and providing security training to all employees were prominent in our discussions. Federal leaders said agencies should seek to reach potential employees who typically are not targeted for



45%

44%

44% of respondents to our survey said they were **"very satisfied"** and 45% **"satisfied"** with their agency's focus on security to support government resilience.

Government already recognized the importance of implementing zero trust security. In 2020, the **Chief Information Security Officers Council** made accelerating the adoption of zero trust security a priority, according to federal leaders. Agencies such as the departments of Education and the Interior, the General Services Administration, the National Oceanic and Atmospheric Administration and the Small Business Administration have adopted zero trust security to some degree.

"Our security team sends fake spam and gives friendly reminders to employees that clicked on a link that they shouldn't have clicked on. It sounds like a small thing but if you are changing culture around cybersecurity or otherwise, culture really is small behaviors, not grand gestures, that are repeated until they are expected."

— Hayri Tarhan, director of solution consulting, U.S. federal civilian, ServiceNow

recruitment for cybersecurity jobs, such as college graduates with degrees other than computer science or even people without degrees who nonetheless possess the required skills.

Cybersecurity professionals who come on board at agencies should then be an integral part of designing and developing new technologies and systems, alongside developers, operators and users, a practice called DevSecOps. This could ensure that technology is built and used with security considerations in mind.

But leaders also asserted that simply hiring and working with cybersecurity experts is insufficient. Rather, all employees should regularly be trained on security and participate in security drills and simulations to learn how to handle cybersecurity threats they might encounter on the job. All project managers in government should understand the role cybersecurity plays in their projects and how to secure the technology tools and devices used in their programs. Small steps can make a difference, with some organizations' security teams using fake spam emails to help employees learn how to distinguish spam from legitimate messages.

Beyond the need for investments in training, leaders discussed how identity authentication is an opportunity to improve security. Identity authentication is the process through which users—whether federal employees or the public—verify their identity and confirm their right to access a technology tool or information network. The need for authenticating many users at once came to the fore during the pandemic. Agencies found ways to ascertain the identity of employees who were increasingly trying to access agency networks from a distance and members of the public who also were increasingly turning to government's digital tools to request or use services. Both groups of users go through the verification process to prove they are not malicious actors using someone else's identity to access agency systems and information.

Agencies have several ways to authenticate identity for remote communication, including requesting photos of an identification document, such as a driver's license; using biometrics, such as fingerprints; confirming personal information, such as a phone number; requesting users reenter a password; or requiring people to enter a PIN unique to them.^{7,8}

Federal leaders also agreed government should continue its move to "zero trust security," which assumes malicious actors constantly threaten information systems and that every part of a network must be secured continuously.

This strict approach boosts security for every device connected to a network. The need to secure individual devices will only grow in importance if more federal employees to continue to work remotely, as expected, using their own devices to connect to agency networks.

Zero trust security moves cyber defenses from a network's perimeter to each individual device—in our homes, this would mean protecting every device connected to our

wireless network every time the device is used, not simply protecting our Wi-Fi network as a whole from outside threats. In a zero trust network, the identity of users is continually authenticated, and users are allowed to access only the parts of the network they need for their jobs.

Another element of zero trust security is automation and the use of advanced tools such as artificial intelligence, participants said. With the emphasis on continuously monitoring all parts of an information network, AI tools that can rapidly complete repetitive tasks can reduce the burden on cybersecurity staff.

Additionally, as cyberattacks and malicious actors proliferate, agencies must deal with an exponentially increasing amount of information about these threats. The amount of data can be overwhelming for security analysts, who must sift through past attacks to fix existing vulnerabilities, keep systems secure in the moment and prepare for future threats. In such an environment, federal leaders said, human analysts simply cannot monitor all the risks and identify the threats most likely to harm government and the entities it serves.

AI tools can analyze large amounts of information and draw analysts' attention to the most serious attacks or most concerning vulnerabilities. AI tools also can constantly monitor the entirety of agency networks and identify potential issues, such as corrupted computer files or manipulated metadata—a set of data that gives information about other data—that might indicate a cyber intrusion. Working alongside AI, analysts can focus their time on real vulnerabilities while the AI monitors routine activity that does not pose a threat.

Top recommendations

Federal agencies should:

- Make employee training a continual focus, not a one-time activity. Run security drills and simulations to help employees learn how to recognize and respond to cybersecurity threats. All project managers should understand the role cybersecurity plays in their projects and how to secure the technology tools and devices used in their programs.
- Embrace a zero trust mindset, which requires verifying anyone trying to access technology systems. This strict approach boosts security for every device and user connected to a network.
- Use artificial intelligence tools to manage an exponentially increasing amount of information about cyber threats. AI tools can analyze large amounts of information that would be overwhelming for security analysts, drawing their attention to the most serious threats and vulnerabilities.

7 General Services Administration, "Login.gov—How to verify my identity." Retrieved from <https://bit.ly/3mfa46L>

8 General Services Administration, "Introduction - PIV Guides." Retrieved from <https://bit.ly/3onjsHe>

CONCLUSION

The COVID-19 pandemic has been a watershed moment for the federal government. Employees have been called on to manage public health and economic crises the coronavirus caused while navigating unprecedented challenges in their own lives. Many people have put their health and safety on the line to protect the health and safety of others. They continue to inspect our food and water and respond to hurricanes and wildfires.

While most agencies are succeeding in moving the mission forward despite the coronavirus, well-documented challenges agencies have faced for years, even decades, have made it more difficult for some of them to muster a successful response. They have struggled with inaccurate public health data, the potential fraud in disseminating of economic stimulus payments and increased cybersecurity threats.

It became clear that America's resilience depends on the federal government's resilience. The coronavirus

pandemic highlighted that our government must have the tools and resources to serve the public even during external shocks and changing circumstances.

Federal agencies must invest in their workforces as a strategic asset, foster a culture of innovation, renew their focus on cybersecurity and purchase the newest technologies. Only sustained investments in workforce, innovation, technology and security can ensure government is ready to face a post-pandemic world and new crises that arise.

Our three organizations—ACT-IAC, MeriTalk and the Partnership for Public Service—along with our private sector partners, conducted this research to help set up leaders in the Biden administration and on Capitol Hill for success. Leaders can learn from agencies that succeeded at managing the pandemic and build a foundation for government's resilience to future crises.

RESILIENCE IN THE PANDEMIC

85%

agree the COVID-19 pandemic is a watershed moment for federal government modernization

67%

agree their agency's resilience improved between January and August 2020, but just

27%

grade it an 'A' today—even after adapting to COVID-19

Less than half of feds are satisfied with their agency's focus on key components of government resilience:



44%
Security



36%
Information technology



29%
Human capital



26%
Innovation

CRITICAL COMPONENTS OF RESILIENT GOVERNMENT

Top challenges in light of the COVID-19 pandemic:



Security:

- #1** Budget constraints
- #2** Legacy infrastructure
- #3** Expanded threat landscape



Information technology:

42% say at least half of the IT they use for work needs to be updated or replaced



Human capital:

85% agree their agency has a workforce skills gap



Innovation:

33% strongly agree their agency encourages them to come up with new and better ways of doing things

BUILDING A RESILIENT FUTURE

What does a resilient federal government look like?



Agile workforce



Ability to adjust to changing customer needs



Culture of preparedness



Cutting-edge cybersecurity



Modern infrastructure, maximizing cloud computing

Most important changes to improve government resilience:

Security:



Provide security training for non-IT workforce



Provide security training for IT workforce



Implement or expand mobile threat defense

Information technology:



Expand remote access



Increase reliability



Increase security

Human capital:



Create a flexible work environment



Accelerate dismissal of poor-performing employees



Invest in workforce retention

Innovation:



Empower employees to be creative



Remove internal barriers to effectiveness



Increase communication around innovation from senior leadership



**PARTNERSHIP
FOR PUBLIC SERVICE**

1100 New York Avenue NW
Suite 200 East
Washington DC 20005

(202) 775-9111
ourpublicservice.org
CFC# 12110

 [partnershipforpublicservice](https://www.facebook.com/partnershipforpublicservice)

 [@PublicService](https://twitter.com/PublicService)

 [rpublicservice](https://www.instagram.com/rpublicservice)



3040 Williams Drive
Suite 500
Fairfax, Virginia 22031

actiac.org

 [act.iac](https://www.facebook.com/act.iac)

 [@ACTIAC](https://twitter.com/ACTIAC)



P.O. Box 1356
Alexandria, Virginia 22313

meritalk.com

 [@MeriTalk](https://twitter.com/MeriTalk)