# Ensuring Continuity, Effectiveness and Security During Uncertain Times

**The New Tomorrow for Civilian Federal Agencies**

Gigamon®

# Executive Summary

Throughout history, the federal government has demonstrated the capabilities, ingenuity, and resiliency to overcome monumental challenges at a large scale. COVID-19 and its aftermath presented an entirely new type of challenge, requiring mobilization of civilian federal agencies to contain an unprecedented crisis while simultaneously transforming where and how key personnel performed their duties.

The impacts of COVID-19 were far-reaching for the 18 U.S. civilian federal agencies,[1] many of which were forced to balance an extensive shift to remote work with essential missions during the crisis. Notable examples include:

+ The Department of Health and Human Services' role in the public health response
+ The Department of the Treasury's administration of a large federal stimulus program
+ The Federal Emergency Management Agency's focused crisis response efforts
+ The State Department's role in administering travel restrictions and international aid efforts

The federal government was already taking steps to modernize its technology infrastructure before the health crisis. However, the need to rethink how civilian agencies work remotely, collaborate and engage with the public forced a rapid acceleration and adaptation of these efforts. It is also driving a more urgent focus on security vulnerabilities. For example, the U.S. Government Accountability Office has identified essential legacy systems in need of modernization to address security risks at the Department of Homeland Security, Department of the Interior, Department of the Treasury, Small Business Administration, Social Security Administration and more.[2] These risks are magnified by the rapid shift to remote work, cloud migration and for some agencies, the convergence of IT with operations technology (OT) and industrial control systems (ICS), increasing the need to accelerate existing security priorities such as moving towards Zero Trust architecture.

# Overview

This paper looks at IT priorities that civilian federal agencies will need to address now and in The New Tomorrow.

### TODAY

The federal government's present imperative is fulfilling public health, economic and crisis response missions with speed and effectiveness while devising and implementing strategies for keeping personnel safe and ensuring continuity of government. These efforts required acceleration of cloud migration and work from home (WFH) capabilities, and now federal IT teams must take the necessary steps to mature and further expand these IT competencies.

### RETURN TO WORK

A significant number of federal government employees were forced to transition to a WFH model in a matter of days with minimal opportunity for advance planning. This put new demands on the government's IT infrastructure. It also created new possible security attack vectors. As civilian agencies transition back to normal operations, they will find a new set of ongoing operational requirements and a growing need to adapt and strengthen their security posture.

### THE NEW TOMORROW

Faced with uncertainty, challenges and opportunities, the federal government must develop constituent services and governing models that cover a number of possible futures, and build an agile network and security infrastructure to support these models. If federal government IT teams act proactively to build a core set of network operations, cloud and security competencies now, they will be well-equipped to adapt as needed during these extraordinary times.

We would like to share our thoughts on how state and local governments can best navigate these challenges and opportunities and equip their NetOps and InfoSec teams to be successful in these unprecedented times.

# Today

Now that the IT teams have addressed the immediate requirements of the COVID-19 crisis, federal government IT teams face a new set of challenges driven by several key imperatives.

## Accelerate Cloud Migration

The federal government's strategy of broader adoption of cloud infrastructure dates back to 2011, when the office of the U.S. Chief Information Officer (CIO) introduced the Federal Cloud Computing Strategy, often referred to as "Cloud First."[3] Cloud First required that agencies pursue cloud options first for any new initiatives before procuring and building out new on-premises IT infrastructure. While some agencies did move in this direction over the last decade, others moved more slowly.

By 2018, with a new strategy underway called "Cloud Smart,"[4] the momentum had begun to build. Nearly half of federal IT executives (48 percent) surveyed at the time indicated that they expected their agency to augment or migrate at least some of their IT infrastructure to the cloud within the subsequent two years.[5] Nonetheless, the U.S. Government Accountability Office estimated in 2019 that only about 17 percent of new civilian agency IT investments leveraged the cloud.[6]

According to the same report, the agencies that did embrace the cloud realized $291 million in cost savings between 2015 and 2019. More importantly, however, the strategic importance of cloud migration was put on display with the rapid shift to a WFH model during the COVID-19 health crisis, as cloud-enabled agencies were in a much better position to adapt. For example, the Department of Homeland Security (DHS) specifically cited earlier cloud migration efforts as the key to its ability to shift more than 70,000 employees to telework rapidly.[7] In FY 2020, the Office of Management and Budget (OMB) reported that cloud investment rose to over $2.2 billion; the top three departments with reported investments were Health and Human Services, DHS and Veterans Affairs.[8]

Throughout the COVID-19 crisis, the Cybersecurity and Infrastructure Security Agency (CISA) has been updating its Trusted Internet Connections (TIC) 3.0 guidance[9] to help agencies develop modern and secure remote productivity capabilities. Initial TIC use case focus areas include:

+ Remote user
+ Infrastructure-as-a-Service (IaaS)
+ Platform-as-a-Service (PaaS)
+ Software-as-a-Service (PaaS)
+ Email-as-a-Service (EaaS)

As these TIC use case priorities illustrate, cloud migration and WFH initiatives are tightly coupled.

## Optimize the Work-from-Home Model

For most federal government agencies, the shift to a WFH model was conducted in weeks, leaving IT teams with little time to plan or scale their remote access infrastructure. Over time, most agencies did eventually stabilize their WFH capability. Many are now focused on optimizing this environment to provide the best possible user experience to their employees while ensuring that agency missions are executed effectively.

As in the private sector, federal WFH capabilities are highly dependent upon video conferencing applications such as Microsoft Teams and WebEx. For example, the use of online collaboration tools by the Department of Education grew six-fold from an average of 60,000 calls per month to over 370,000 as most employees shifted to a remote work model.[0]

While these apps are SaaS-based and can scale rapidly, they can place a heavy load on network bandwidth, often resulting in a poor user experience. Additionally, the way that departments and individuals use these apps may pose potentially serious security issues.

It is vital for security and network teams to find ways to work more efficiently and extend the life of their existing tools and infrastructure.

The need for access to on-premises applications also led to a load spike on the virtual private network (VPN) infrastructure used by agencies. For example, even as the Department of Education leveraged SaaS infrastructure for collaboration as noted above, they saw VPN infrastructure utilization jump from 20 to 25 percent to the upper 90s percentage range.[10]

One of the recent updates that CISA made to TIC 3.0 was the issuance of interim telework guidance to help agencies manage the large spike in remote work.[11] In addition to outlining possible technology approaches, this updated guidance emphasizes the importance of maintaining visibility and cybersecurity monitoring capabilities as IT workloads migrate to the cloud and users work from more locations.

## Accomplish More with Less

Agency budgets are now being challenged by new requirements and security needs as a result of the health crisis and related workflow transformations. Growing security threats from adversarial nation-states, cybercriminals, disgruntled employees and other bad actors seeking to exploit the crisis are placing further pressure on budgets at all levels of government. In short, the pressure to do more with less is greater than ever. It is vital for security and network teams to find ways to work more efficiently and extend the life of their existing tools and infrastructure.

There is some short-term financial relief for some agencies, most notably $4.6 billion in funding that was included in the CARES Act to support federal agency telework and telehealth initiatives.[12] The most successful agencies will be the ones that use this budget infusion to invest in cloud, IT modernization, WFH and related security measures that will enable innovation and agility even if federal IT budgets shrink over time once the immediate health crisis has passed.

# Return to Work

Today, most civilian agencies are navigating an uncertain set of requirements. As stay-at-home orders are gradually relaxed, many agencies are bracing for additional periods of disruption. This requires a careful balancing act of restoring traditional in-person functions while continuing to invest in technologies to support remote work and online government services. In addition, many unplanned positive outcomes were realized during the forced WFH period, including increased productivity and higher satisfaction in some roles. This will likely lead to higher sustained levels of WFH activity even when it is no longer necessary for health and safety reasons.

A more permanently distributed federal workforce increases the importance to adopt Zero Trust principles, and for several civilian agencies, a need to focus on enhancing the security posture of ICS and OT networks.

Finally, as the federal government IT infrastructure evolves into a heterogenous blend of on-premises and cloud infrastructure, it is essential to have a strategy to achieve and maintain the necessary visibility to aid in both security and performance assurance.

## Accelerate Zero Trust Adoption

Independent of the COVID-19 crisis, the federal government has identified Zero Trust as a key security model that will help enable IT modernization and cloud migration while minimizing security risk. According to NIST Special Publication 800-207, Zero Trust Architecture, Zero Trust security models "assume that an attacker is present in the environment and that an enterprise-owned environment is no different — or no more trustworthy — than any nonenterprise-owned environment."[13] To implement Zero Trust, an agency's network must be able to analyze data across an environment in near real time, determine the appropriate action based on that analysis, and feed that assessment to a decision point where trust is granted or denied at scale with minimal latency.

Although the Zero Trust concept is not new, most federal agencies are at the beginning of their Zero Trust journeys. As network and security architects grapple with the challenge and complexity of continuously evaluating every user and device that seeks to access network resources and data, they will need to give careful consideration to the back-end capabilities necessary to bring their Zero Trust technologies together into a cohesive and scalable architecture. Three fundamental areas that must be part of these architectures are:

+ Discovery: Achieving clear visibility into all information in motion on the network
+ Data control implementation: Understanding application activity in detail and implementing micro-perimeters, policy enforcement and continuous authentication capabilities
+ Monitoring, detection and response: Implementing a monitoring plane that is capable of seeing all traffic, detecting threats and initiating rapid response

## Secure OT Networks and Industrial Control Systems

One of the major lessons from the COVID-19 crisis is that moving too slowly with IT modernization comes with a cost, as modern IT capabilities enable more nimble and effective responses to unplanned crises. As civilian federal agency IT teams return to normal modes of operation, it is of priority for them to look ahead to the next possible crisis and take proactive mitigation steps.

For certain civilian agencies, such as the Department of Energy and Department of Transportation, ICS and OT network security is another area where modernization plans have been underway but are not moving fast enough in many cases to head off a possible future crisis. ICS and OT networks are often comprised of aging distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems that weren't designed with the modern security threat landscape in mind. These systems are central to the operation of mission-critical capabilities such as controls for utilities, dams, interconnected aircraft systems, navigational systems, power control systems, embedded ground systems, access controls systems and more. As such, availability, including 100 percent uptime requirements in many cases, and safety are top priorities. With the convergence of OT controls with IT networks, there is greater exposure to cyberattacks. Any security compromise could have catastrophic consequences. Therefore, incorporating these systems into a holistic security strategy is essential.

## Ehance Network Visibility and Performance

Faced with the combined pressures of supporting on-site workers, remote workers and citizens accessing services online, federal IT teams will require added visibility into infrastructure performance and tools at their disposal to diagnose and correct issues quickly. This is particularly importance for agencies that were forced to pause or scale back capabilities during the crisis and now face a backlog of demand. In both direct engagement and self-service interactions, harnessing technology to restore public confidence will be essential.

In addition to bolstering essential IT resources, IT teams must also find ways to tune out noise that can overwhelm both tools and personnel. For example, as the use of video conferencing services rises, the impact on network infrastructure and monitoring tools is significant. IT teams must find ways to prefilter high-volume traffic that poses a low level of risk to reduce the burden on network infrastructure and tools.

When application performance issues do arise, it is often necessary to look beyond network bandwidth issues that can be observed by, for example, frame rates slowing or quality dropping from HD to SD, to understand what is happening in the interaction between the application and the network. In these cases, the ability to use the metadata within the application is beneficial in determining where potential bottlenecks or other issues exist that cause poor application performance and user experience.

Agencies that thrive will be resilient, innovative and forward-looking. They will develop operational models that can respond quickly to changing public needs, and they will have IT infrastructures that mirror these core values.

# The New Tomorrow

Many forward-thinking civilian agencies are already looking beyond today's crisis recovery situation and re-imagining the way they serve the public in what people are calling the New Normal, the Next Normal or The New Tomorrow.

As in any period of turmoil and uncertainty, The New Tomorrow will bring new challenges and opportunities. While the degree of change, challenge and opportunity will vary based on the mission, resources and risk tolerance of individual agencies, those that thrive in The New Tomorrow will share a number of characteristics in their cultures, operational models and supporting infrastructures. These agencies will be resilient, innovative and forward-looking. They will develop operational models that can respond quickly to changing public needs, and they will have IT infrastructures that mirror these core values.

## ✓ VISIBILITY

You can't manage what you can't see, so gaining visibility into all network traffic across both IT and OT infrastructure will become a survival issue for many civilian agencies. The physical, virtual and cloud-based visibility into both encrypted and unencrypted data that Gigamon provides is already trusted by many of the world's most demanding organizations, including many government agencies and private sector businesses.

## ✓ AGILITY

As recent events have shown, agility doesn't just mean handling the pressures of growth and innovation; it also means handling unforeseen and unprecedented change. In this situation, it is critical that civilian federal agencies' networks and security capabilities support continued changes in working practices, community infrastructure usage and new tools deployment.

## ✓ GROWTH

Many agencies will need to significantly upgrade their networks as they deliver new online experiences to the communities they serve, evolve their digital capabilities and embrace emerging technologies such as IoT. In addition to these growth drivers, many government leaders will rethink and reorganize departments and agencies based on lessons learned during the crisis, a process that will drive the need for network consolidation.

## ✓ CLOUD

For time-to-deployment and scalability reasons, the cloud is the preferred application deployment platform for The New Tomorrow. This will include both SaaS-based applications and custom applications running on IaaS or PaaS infrastructure. As cloud adoption accelerates, maintaining visibility into all information — regardless of whether it is on-premises or in the cloud — and having the ability to manage and secure it, will become an increasingly important mandate for federal agencies.

## ✓ COST EFFICIENCY

Civilian agencies cannot rely on sizable budget increases to address the challenges of The New Tomorrow. Keeping pace with rapidly evolving workflows, performance requirements and security challenges will only be possible if federal IT teams can find ways to unlock new efficiencies from existing tools. Eliminating unnecessary traffic processing demands, offloading resource-intensive functions like decryption from individual tools, and centralizing NetOps, CloudOps and InfoSec management functions under a single pane of glass for greater efficiency are a few strategic steps that agencies can take to meet new challenges while reducing costs.

# Final Thoughts

The COVID-19 crisis has set off a chain reaction of events that will profoundly affect our society and economy for the foreseeable future. Leadership and innovation at the federal government level can play a transformative role in the public health and economic posture of the United States. In the short term, performing essential government services as effectively as possible is of utmost priority. However, many opportunities exist to apply the lessons learned from this crisis to improve how the federal government can serve its citizens, as well as mitigate the impact of future crises. Meeting immediate needs while taking full advantage of the opportunities that lie ahead will require resilience, agility and visibility in every aspect of governmental operations, including networks and information security systems.

# About Gigamon

Gigamon provides network visibility and analytics on all traffic across your physical, virtual and cloud networks to solve critical security, performance and business continuity needs. The Gigamon Visibility and Analytics Fabric™ delivers optimized network and security performance, simplified management and accelerated troubleshooting while increasing your tools' return on investment. Our comprehensive solutions accelerate your organization's ability to detect and respond to security threats, including those hidden in encrypted traffic. Trusted by 83 percent of the Fortune 100 and 4,000 organizations worldwide, deployed by ten out of the top ten U.S. federal agencies, governments and educational institutions at all levels globally, Gigamon ensures that your organization can run fast and stay secure in The New Tomorrow.

**For the full story on how Gigamon can help you, please visit gigamon.com.**
**See what our customers are saying.**

Gigamon®

**Worldwide Headquarters**
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

[1] Agency Profiles. FedCyber.
http://www.fedcyber.com/agency-profiles/civilian-agencies/.

[2] "Agencies Need to Develop Modernization Plans for Critical Legacy Systems." Government Accountability Office. Publication GAO-19-471. June 11, 2019.
http://www.gao.gov/products/GAO-19-471#summary.

[3] "Federal Cloud Computing Strategy." The White House Archives: President Barack Obama. February 8, 2011.
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[4] "From Cloud First to Cloud Smart." Federal Cloud Computing Strategy. Office of the Federal Chief Information Officer.
https://cloud.cio.gov/strategy/.

[5] Phil Goldstein, "What Impediments Remain for Federal Cloud Adoption?" FedTech. January 22, 2019.
http://fedtechmagazine.com/article/2019/01/what-impediments-remain-federal-cloud-adoption.

[6] "Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked." April 2019. U.S. Government Accountability Office. Publication GAO-19-58.
https://www.gao.gov/products/GAO-19-58.

[7] Jane Edwards. "Beth Capello: Cloud Migration Paying Dividends for DHS." May 27, 2020.
http://www.executivegov.com/2020/05/beth-cappello-cloud-migration-paying-dividends-for-dhs.

[8] "Federal Cloud Computing Market, 2020–2022." GovWin, Deltek. August 27, 2020.
https://iq.govwin.com/neo/marketAnalysis/view/Federal-Cloud-Computing-Market--2020-2022-/46722?researchTypeId=2&researchMarket.

[9] "Trusted Internet Connections." U.S. Cybersecurity and Infrastructure Security Agency.
http://www.cisa.gov/trusted-internet-connections. Accessed September 28, 2020.

[10] "CIO Crossroads: Federal IT in the COVID Crisis – Education Department Edition." MeriTalk. July 22, 2020.
http://meritalk.com/articles/cio-crossroads-federal-it-in-the-covid-crisis-education-department-edition.

[11] "Trusted Internet Connections 3.0 Interim Telework Guidance." April 8, 2020. U.S. Cybersecurity and Infrastructure Security Agency.
https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf.

[12] Alex Rossino. "Stimulus Funding for Telework and Telehealth in the CARES Act." March 30, 2020.
http://iq.govwin.com/neo/marketAnalysis/view/Stimulus-Funding-for-Telework-and-Telehealth-in-the-CARES-Act/4049.

[13] S. Rose, O. Borchert, S. Mitchell, and S. Connelly. "Zero Trust Architecture." August 2020. National Institute of Standards and Technology, U.S. Department of Commerce. NIST Special Publication 800-207.
https://doi.org/10.6028/NIST.SP.800-207.