Government Business Council

ISSUE BRIEF

NETWORK READY

Strengthening IT Systems to Optimize Nationwide Services

SPONSORED BY: ciena | WINDSTREAM ENTERPRISE

THE BIG ISSUE

While the federal government is tasked to meet the nation's most daunting challenges, agencies continue to use outdated legacy IT systems meant to support their missions. From the uptick in service demand to the rise in network activity, agency networks and systems face significant pressure in the time of COVID-19 and beyond.

WHY IT MATTERS

Without the proper IT, government agencies jeopardize their ability to fulfill and deliver services needed most by everyday citizens.

Legacy IT

Shows Its Weak Spots

1

STRAINS FROM CONSUMER TRAFFIC

During national and state emergencies, government agencies have faced difficulties processing the surges of service demand. In April 2020, for example, 10 million people filed for unemployment in just two weeks, which is about 15 times more than the unemployment claims made in a week during the Great Depression.[1] Several states' unemployment systems crashed during these spikes in user activity, as they were unable to handle the traffic.[2]

The Small Business Administration's (SBA) electronic loan processing and computer systems also experienced a crash earlier this year, resulting from a dramatic increase in loan applications from small businesses.[3] Under normal circumstances, SBA's system handles about 60,000 loans annually; this year, it received over a million applications, causing cascading problems with delivering services to those who need them most.[4] Agencies will need to bolster their IT infrastructure to be prepared for similar instances of future heightened demand.

2

THE HEAVY HAND OF TELEWORK

With increased telework demand, agencies are experiencing issues with bandwidth on their networks. The Navy, for example, has only a limited capacity on its internal network for simultaneous connections to Virtual Private Networks (VPNs),[6] despite having the second highest population of active-duty personnel of all military services.[7] To respond to its limited network capacity, the Department of Defense (DoD) sorted teleworkers into three categories prioritized by need of accessing internal networks.[8] Additionally, the Department blocked streaming services on its network to maintain capacity for critical services.[9]

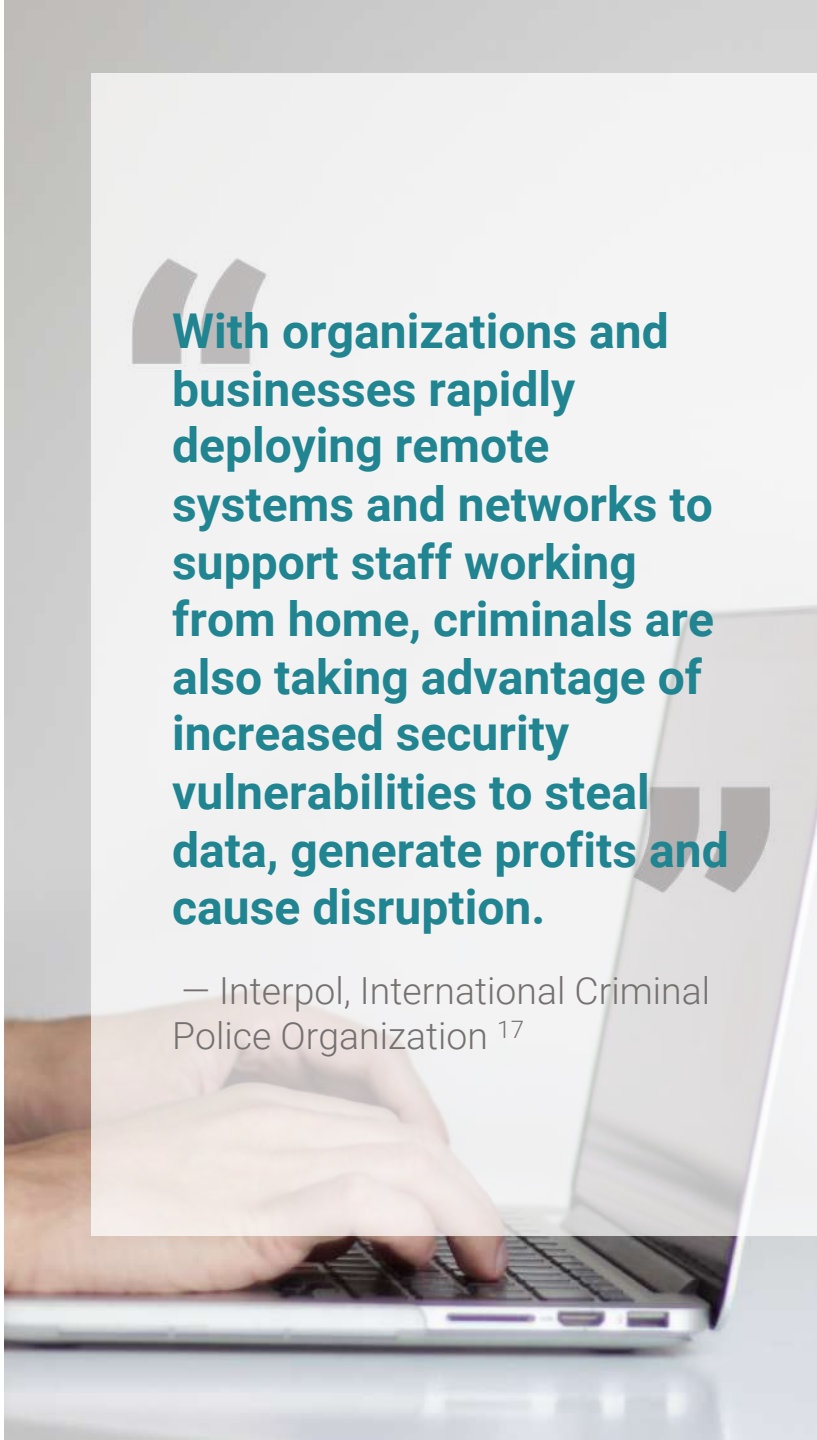
Other agencies, such as the Department of Energy's (DOE) Office of Environmental Management, adjusted work hours to minimize pressure on networks.[10] Likewise, the Office of Personnel Management (OPM) resorted to rolling back non-essential functions that were responsible for overloading its network capacity.[11] As these examples show, it is vital that agencies equip their teams with high-capacity networks to accommodate both in-office and out-of-office work needs.

3

INCREASED NUMBER OF CYBER ATTACKS

Government's dispersed network has dramatically increased vulnerabilities of government agencies to cyber attack. The DoD, for example, has seen a tremendous uptick in cyber attacks during COVID-19.[13] Earlier this year, the Cybersecurity and Infrastructure Security Agency (CISA) issued a warning pertaining to the rise in cyber-attacks perpetrated against remote workers.[14]

Further compounding the issue, ten of the government's most critical legacy systems face moderate to high security risks, including several systems aged over 40 years old.[15] Additionally, most federal agencies have not met the cybersecurity requirements laid out in the Federal Cybersecurity Workforce Assessment Act of 2015.[16] Agencies would benefit from pursuing enhanced cybersecurity for their networks, especially as cyber threats continue to emerge.



"With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption."

— Interpol, International Criminal Police Organization [17]

AGENCY RESPONSE

Some agencies are taking effective steps to respond to impacts on the network

U.S. Small Business Administration

The SBA responded to problems with its loan processing system by increasing processor memory, improving technology, and establishing a pacing mechanism for loan applications.[18]

The Department of Transportation (DoT) is rethinking network cybersecurity. Networks are now dispersed, which means looking at different cybersecurity controls and networks (such as SD-WAN networks).[19]

The Department of Homeland Security (DHS) is increasing its cybersecurity protections for the Centers for Disease Control and Prevention (CDC) and Department of Health and Human Services (HHS) by regularly scanning their devices connected to the Internet.[20]

With a vast network of over 2,100 locations, the National Oceanic and Atmospheric Administration (NOAA) is looking to modernize its older infrastructure to provide high-quality services to sites across the country.[21]

The National Endowment for the Arts (NEA) has focused on increasing the capacity of their management systems to process large volumes of grants. [22]

The Air Force increased its network bandwidth by tenfold compared to its pre-COVID capacity levels. [23]

The Defense Information Systems Agency (DISA) upgraded its Defense Information Systems Network (DISN) to a network 10 times faster than its older 10 GB/s network, creating robust connectivity for combatant commands. [24]

What Now?

What are some next steps agencies can take to strengthen their IT infrastructure to provide mission critical services?

INCREASE NETWORK BANDWIDTH

Adequate network capacity is fundamental to government fulfilling its mission-critical work. However, agencies are heavily reliant on VPNs with telework and may have limited bandwidth between VPNs and internal networks. Some organizations have taken steps to increase bandwidth to meet employee needs. For example, the Army has increased its network bandwidth by four times to support its 800,000 employees working from home.[25] Expanding network capacity can help ensure that technology supports agency missions, not hinder them.

BOLSTER NETWORK CYBERSECURITY

With cyber attacks on the rise, government agencies must keep pace with the frequency and complexity of cyberthreats. In addition to cybersecurity technology, agencies should consider adopting cyber-hygiene practices and security models, such as Zero Trust and Continuous Diagnostics and Mitigation (CDM). Thinking beyond the technology is vital for agencies looking to secure their networks from all angles.

REPLACE OUTDATED SYSTEMS THAT LACK NECESSARY CAPACITY

Outdated technology needs to go. The IRS, for example, has the oldest IT systems in the government, dating back to the 1960s.[26] These systems are unable to keep pace with the amount of electronic work being processed today, and agencies should adopt more agile technologies that can progress at the same rate as the rapid development of software. Cloud computing, for instance, enables agencies to acquire new applications to meet the evolving needs of their agency. If agencies face limited IT budgets or constraints on an IT overhaul, they might benefit from network upgrades that include network elements, but allow older protocols to be natively supported.

ENDNOTES

1. https://www.brookings.edu/research/unemployment-insurance-is-failing-workers-during-covid-19-heres-how-to-strengthen-it/
2. https://www.cbsnews.com/news/coronavirus-unemployment-claims-crash-websites/
3. https://www.nytimes.com/2020/04/27/business/sba-loan-system-crash.html
4. https://www.nbcnews.com/business/business-news/thousands-applicants-zero-loans-trump-s-small-businesses-lending-program-n1176766
5. https://www.gao.gov/reports/GAO-20-625/#TOC_Letter_Findings
6. https://news.usni.org/2020/03/19/navy-dod-networks-strained-under-telework-demand-leaders-ask-limit-use-of-reply-to-all
7. https://www.cfr.org/backgrounder/demographics-us-military
8. https://federalnewsnetwork.com/defense-main/2020/03/as-pentagon-gears-up-for-more-teleworkers-its-networks-already-feeling-the-strain/
9. https://federalnewsnetwork.com/defense-main/2020/03/as-pentagon-gears-up-for-more-teleworkers-its-networks-already-feeling-the-strain/
10. https://www.fedscoop.com/agency-bandwidth-maximum-telework/
11. https://www.opm.gov/our-inspector-general/publications/response-to-covid-19/covid_19_top_management_challenges.pdf
12. https://www.defenseone.com/threats/2020/03/attacks-dod-networks-spike-telework-brings-unprecedented-loads/163812/
13. https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update
14. https://www.gao.gov/assets/700/699616.pdf
15. https://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study#t=0
16. https://abcnews.go.com/Politics/alarming-rate-cyberattacks-aimed-major-corporations-governments-critical/story?id=72164931
17. https://www.gao.gov/reports/GAO-20-625/#TOC_Letter_Findings
18. https://www.meritalk.com/articles/cio-crossroads-dot-edition/
19. https://www.cyberscoop.com/coronavirus-cybersecurity-dhs-cisa-bryan-ware/
20. https://federalnewsnetwork.com/technology-main/2020/07/noaas-next-generation-of-network-infrastructure/
21. https://www.opm.gov/our-inspector-general/publications/response-to-covid-19/covid_19_top_management_challenges.pdf
22. https://www.bizjournals.com/washington/news/2020/04/13/coronavirus-accelerates-pentagon-network-upgrades.html
23. https://www.disa.mil/NewsandEvents/2018/DISA-Network-Upgrade
24. https://www.bizjournals.com/washington/news/2020/04/13/coronavirus-accelerates-pentagon-network-upgrades.html
25. https://www.nextgov.com/it-modernization/2018/03/irs-system-processing-your-taxes-almost-60-years-old/146770/

Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at: www.govexec.com/insights

WINDSTREAM ENTERPRISE

Windstream Enterprise is a managed communications services provider, delivering nationwide, cloud-optimized network and industry-leading services—such as SD-WAN and UCaaS—through our award-winning portal, WE Connect.

Learn more at:
www.windstreamenterprise.com/fed-gov

ciena®

Ciena. Advancing 21st century missions with trusted, reliable, and secure networking solutions.

Cyber security. Automation. Agile service delivery. Key components to mission success, and critical needs for agencies modernizing their network infrastructure. Budgets however are standing in the way of progress: Many agencies struggle to balance their need to deliver new services with the cost of supporting legacy applications and infrastructure. A simpler network infrastructure that supports both legacy and modern technology is required to accelerate mission response. Modernizing IT and communications infrastructure can enable automation, improve performance, and assure cyber resiliency.

Learn more at: www.ciena.com/government


Government
Business
Council
ciena
WINDSTREAM
ENTERPRISE