White Paper: Networks of the Future

Executive Summary

The purpose of this white paper is to provide Federal Government CIOs insight into the next generation of network technologies and how they will impact agencies. Computer networks are fundamental to all information technology and the digital economy. The ways in which agencies manage and secure their networks will change in the near future as network technologies evolve to provide new services and meet increasing data demands. This paper provides a high level overview of the technologies and policies that affect network modernization and security and also provides several recommendations to agencies based on discussions with networking subject matter experts throughout the Federal Government. Suggested actions include: (1) surveying the technology landscape and understand market offerings; (2) incorporating pilots and knowledge sharing into existing network modernization strategies; (3) investing in upskilling of network managers to take advantage of emerging technologies, such as SD-WAN; and (4) collaborating with GSA and other stakeholders to meet acquisition milestones. The future of networks is one of ubiquitous connectivity, greater speeds, and more connected devices that will enable new services to customers and citizens.

Introduction

Technology trends in enterprise computing are testing the limits of existing network architectures. With the consumerization of IT, mobility, and virtualization, applications are increasingly moving to cloud environments; developers are increasingly using open-source software, containers, microservices, and serverless computing platforms; and Federal employees and customers expect instant connectivity on mobile and personal devices. The deployment of low earth satellites could provide broadband connectivity to rural and underserved markets in the United States and most areas of the globe. Network modernization will be at the heart of the new digital economy and tomorrow's government. In the coming years, emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML), new industrial sensors and the proliferation of Internet of Things (IoT) devices, and the rise of the mobile workforce will require new approaches to manage, automate, and secure agencies' networks. The two most significant networking trends on the horizon are the emergence of 5G mobile networks, which will fundamentally change mobile and computing on the edge, and the increasing adoption of Software Defined Wide Area Networking (SD-WAN), which will change how networks are managed and operated for IT enterprises.[1]

The Emerging 5G Landscape

The emergence of fifth-generation (5G) mobile networks promises to fundamentally change how companies, citizens, and government agencies interact with technology. 5G will enable the next generation of consumer and industrial technologies, such as autonomous vehicles, smart grid technology, industrial sensors, Internet of Things (IoT) devices, real-time Augmented Reality (AR), remote surgery, advanced robotics, and precision agriculture systems.[2] In addition to next generation technologies, one of

[1] From conversations with Network and Telecommunications SMEs at GSA on 20 May 2019.
[2] Robinson, Scott. The impact of 5G technology on security and network management. 18 Feb 2019. https://www.cisco.com/c/en/us/solutions/enterprise-networks/impact-of-5g-technology.html

the most innovative aspects of 5G network architecture will be its reliance on 5G network slicing. Network slicing is a type of virtual network architecture that allows virtual networks to exist on top of shared physical infrastructure. This means that network resources can be dynamically allocated to meet technical and services requirements with respect to throughput, latency, reliability, and availability.[3]

More users using more data on more devices are the factors driving increasing demand for improved mobile networks.[4] Gartner estimates that by 2020, there will be over 20 billion IoT devices serving consumers and businesses[5] and some analysts predict that the 5G market will create up to 3 million new jobs in the United States and add up to $500 billion to the nation's GDP.[6] Along with economic benefits, the amount of personal information available for exploitation will increase exponentially and raises concerns from privacy and security professionals.[7] The Federal Government must weigh the economic benefits of 5G deployment with issues such as data privacy, rural accessibility, and national security and counterintelligence concerns.

While the Federal Government has a critical role to play in the rise of 5G, telecommunication companies, hardware manufacturers, and governments around the world will take part in defining the technology standards that make up 5G mobile network technology. The previous shift in mobile communications technology, from 3G to 4G, occurred around 2010 and enabled technologies consumers and government agencies rely on daily, such as Voice over IP (VoIP), Internet Protocol version 6 (IPv6), real-time video conferencing and streaming capabilities, and true mobile broadband on smartphones, tablets, and laptops. Although there is no universal standard yet, 5G networks will offer increased bandwidth and capacity, speeds up to 100 times faster than 4G networks, constant connectivity, and lower latency. The 3rd Generation Partnership Project (3GPP) is the international standards setting organization responsible for developing the technical specifications, standards and requirements for 5G mobile networks around the world.[8] In the United States, private industry is leading deployment efforts, with Verizon, AT&T, T-Mobile, Sprint, and other carriers releasing 5G services in 2019 and 2020.[9]

Rolling out 5G networks, in both cities and rural areas, means rebuilding much of the United States' cell networks and switching systems, which requires close coordination between federal, state, and local governments. The Trump Administration is focused on positioning the United States as a world leader in global 5G readiness. In remarks on April 12, President Trump stated, "secure 5G networks will absolutely be a vital link to America's prosperity and national security in the 21st century. 5G will be as much as 100 times faster than the current 4G cellular networks. It will transform the way our citizens work, learn, communicate, and travel. It will make American farms more productive, American manufacturing more

[3] Rost, P. et al. Network Slicing to Enable Scalability and Flexibility in 5G Mobile Networks. https://arxiv.org/ftp/arxiv/papers/1704/1704.02129.pdf

[4] Gallagher, Jill C. and Michael E. DeVine. Congressional Research Service. Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. 30 Jan 2019. https://fas.org/sgp/crs/misc/R45485.pdf

[5] van der Meulen, Rob. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. 07 Feb 2017. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[6] Accenture Strategy. Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities. 2017. https://api.ctia.org/docs/default-source/default-document-library/how-5g-can-help-municipalities-become-vibrant-smart-cities-accenture.pdf

[7] Gallagher, Jill C. and Michael E. DeVine. Congressional Research Service. Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. 30 Jan 2019. https://fas.org/sgp/crs/misc/R45485.pdf

[8] 3rd Generation Partnership Project (3GPP). https://www.3gpp.org/about-3gpp

[9] Fisher, Tim. When Is 5G Coming to the US? 31 July 2019. https://www.lifewire.com/5g-availability-us-4155914

competitive, and American healthcare better and more accessible "[10] Implementing 5G across the United States will be a multi-year effort with much of the infrastructure and licensing investment coming from private industry.

Currently, the General Services Administration (GSA) Office of Information Technology Category (ITC) is preparing additional resources for agencies interested in learning more about implementing, deploying, and delivering 5G technologies.[11]

Geopolitical Considerations

Three countries are leading the race to deploy 5G technologies:The United States, China, and South Korea. China has assumed a top-down, centralized approach and is leading the world on infrastructure deployment. South Korea has already auctioned 5G spectrum and is committed to being the first to deploy 5G technologies nationwide. The United States has assumed a bottom-up, market-based approach to 5G deployment, with a focus on reducing regulatory barriers for 5G cell siting. However, the lengthy spectrum allocation process, competing demands for spectrum, and local resistance to new 5G regulations may slow deployment in the United States.

In the United States, the race to 5G involves major telecommunications carriers, such as Verizon, AT&T, T-Mobile, and Sprint, as well as hardware providers that manufacture the equipment and technology required to build 5G infrastructure. The Trump Administration considers some foreign hardware manufacturers to be national security threats. In an Executive Order, signed on May 15, 2019, the Trump Administration placed an acquisition ban on information and communications technologies or services designed, developed, manufactured, or supplied by foreign adversaries.[12]

Federal agencies should be cognizant of the latest Administration actions on limiting and restricting foreign firms' ability to deploy 5G and other network technology and equipment in the United States. Agencies undergoing network modernization efforts should also prioritize supply chain assurance, to ensure no network equipment poses a national security threat, and begin implementing security approaches, such as Zero Trust and continuous authentication and monitoring to reduce risks associated with network upgrades.[13]

Rural Broadband Connectivity

Accompanying the Trump Administration's goal of being a global leader in 5G readiness, the Administration has also set the priority of connecting rural communities around the country. President Trump has stated, "as we are making progress with 5G, we're also focused on rural communities that do

[10] Remarks by President Trump on United States 5G Deployment. 12 April 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/

[11] Zielinski, Bill. Way Beyond Wireless: Planning for 5G. 30 July 2019. https://gsablogs.gsa.gov/technology/2019/07/30/way-beyond-wireless-planning-for-5g/

[12] Executive Order on Securing the Information and Communications Technology and Services Supply Chain. 15 May 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

[13] A comprehensive list of policy recommendations and suggested agency actions is presented at the end of this white paper.

not have access to broadband at all…We're working closely with federal agencies to get networks built in rural America faster and at lower cost."[14] According to the FCC's 2018 Broadband Deployment Report, due to the challenges of providing mobile broadband coverage in rural areas, only 70% or rural American and less than 64% of residents in Tribal lands had access to 4G LTE, leaving approximately 15.2 million rural residents without access to mobile broadband services.[15] This means that rural Americans struggle to reach full productivity in the workplace, obtain a modern education, and acquire access to healthcare services.[16]

Although 5G technology will enable super fast wireless connectivity to primary densely populated urban areas in the near future. Much of the country's rural communities do not currently have the infrastructure to support 5G or wired broadband. While major carriers are expected to begin deploying 5G wireless technologies in many cities throughout the U.S. in 2019 and 2020, the Federal government will likely have a significant role to play in ensuring broadband connectivity for more rural parts of the country. The U.S. Department of Agriculture has begun deploying up to $600 million in loans and grants to help build broadband infrastructure in rural America.[17] Furthermore, the NTIA released a report in February 2019 that outlines a vision for how the Federal Government can increase broadband access for all Americans.[18] Additionally, emerging technologies, such as the deployment of low earth satellites could provide broadband to all Americans in the coming years.

Spectrum Allocation

Spectrum allocation is also a driving factor in 5G deployment in the United States and around the world. Spectrum refers to the radio frequencies on the electromagnetic spectrum used to communicate information wirelessly. In the United States, the Federal Communications Commission (FCC) manages spectrum allocation for non-federal users while the National Telecommunications and Information Administration (NTIA) manages spectrum for federal users.[19] 5G leverages low-, medium-, and high-band frequencies on the electromagnetic spectrum. High-band frequencies, also known as millimeter wave spectrum (MMW), offer ultra-fast communication services to high-density areas, such as major cities or campuses. Low-band frequencies offer more broader coverage over greater distances and can penetrate solid objects, such as buildings, more effectively than higher bands.[20]

The Trump Administration has focused on 5G planning, including freeing spectrum for 5G use. On October 25, 2018, President Trump signed a Presidential Memorandum calling for a National Spectrum Strategy to assess current and future spectrum needs and support the deployment of 5G through incentives and reduced regulations. President Trump has stated, "to accelerate and incentivize [5G] investments, my administration is focused on freeing up as much wireless spectrum as needed...and

[14] Remarks by President Trump on United States 5G Deployment. 12 April 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/
[15] Ibid.
[16] Ibid.
[17] U.S. Department of Agriculture Press Release. USDA Launches New Program to Create High-Speed Internet e-Connectivity in Rural America. 13 Dec 2018. https://www.usda.gov/media/press-releases/2018/12/13/usda-launches-new-program-create-high-speed-internet-e-connectivity
[18] American Broadband Initiative. Milestones Report: February 2019. https://www.ntia.doc.gov/files/ntia/publications/american_broadband_initiative_milestones_report.pdf
[19] Gallagher, Jill C. and Michael E. DeVine. Congressional Research Service. Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. 30 Jan 2019. https://fas.org/sgp/crs/misc/R45485.pdf
[20] Federal Communications Commission. The FCC's 5G FAST Plan. https://www.fcc.gov/5G

removing regulatory barriers to the buildout of networks."[21] The FCC is currently in the process of freeing spectrum for 5G use. However, the United States has a complex spectrum allocation process that requires a lengthy rulemaking procedures, an auction process, and a relocation process.[22] Furthermore, additional challenges, such as freeing spectrum without interfering with first responders networks, public safety, or other critical applications, has remained a challenge.[23] Industry advocates have urged policymakers to plan, collaborate, and set timelines to expedite the availability of spectrum, and coordinate spectrum auctions so providers can plan spectrum acquisitions and deployments in 2019 and 2020.

Small Cell Siting

5G will rely on technologies that use a broad range of spectrum frequencies. 5G systems using low- and mid-band spectrum can install new 5G equipment on existing 4G cell sites. This will increase the speed and functionality of existing 4G networks, but will likely not achieve the ultra-fast speeds provided by millimeter wave (MMW) bands. For deployments that leverage higher bands, particularly above 6 GHz, a much higher density of cell sites is needed because the signals cannot travel large distances or penetrate obstacles. To overcome these challenges, providers will place many smaller cell sites close together to relay signals further distances and around obstacles. These small cells are low-powered radio access nodes with ranges between 10 meters to two kilometers and can be installed on existing infrastructure such as buildings, poles, and streetlights.[24] In the United States, constructing new wireless towers or attaching new equipment to pre-existing infrastructure generally requires providers to obtain approval from federal, state, and local authorities, which can further slow approval processes. On September 26, 2018, the FCC approved new rules aimed at facilitating the deployment of wireless infrastructure for 5G networks, which, among other things, limited how states could regulate small cell citing and limited the fees state and local governments could charge on service providers, all in an effort to accelerate 5G small cell installations.[25] Many local governments oppose the FCC ruling, arguing that the rules exceed FCC's authorities, and preempt local authorities to manage public property, protect public health and safety, and manage small cell installation.[26] Another factor that worries state and local governments is the maintenance of 5G infrastructure. More cell sites and more infrastructure means increased operations and maintenance costs to maintain the 5G network and continue providing services. Additionally, 5G will require more complex maintenance with newer hardware. Many parts of the United States may not have enough qualified service personnel, especially early on, leading to coverage outages.[27]

---

[21] Remarks by President Trump on United States 5G Deployment. 12 April 2019. https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/

[22] Gallagher, Jill C. and Michael E. DeVine. Congressional Research Service. Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. 30 Jan 2019. https://fas.org/sgp/crs/misc/R45485.pdf

[23] Gallagher, Jill C. Congressional Research Service. The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress. 27 April 2018. https://fas.org/sgp/crs/homesec/R45179.pdf

[24] Gallagher, Jill C. and Michael E. DeVine. Congressional Research Service. Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. 30 Jan 2019. https://fas.org/sgp/crs/misc/R45485.pdf

[25] Federal Communications Commission. FCC Facilitates Wireless Infrastructure Deployment for 5G. 27 Sept 2018. https://www.fcc.gov/document/fcc-facilitates-wireless-infrastructure-deployment-5g

[26] Gallagher, Jill C. and Michael E. DeVine. Congressional Research Service. Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress. 30 Jan 2019. https://fas.org/sgp/crs/misc/R45485.pdf

[27] Robinson, Scott. The impact of 5G technology on security and network management. 18 Feb 2019. https://www.cisco.com/c/en/us/solutions/enterprise-networks/impact-of-5g-technology.html

Agency Network Modernization

While the emergence of 5G technologies will fundamentally change consumer and industrial wireless network technologies, the next generation of Wi-Fi, known as Wi-Fi 6, will similarly change mobile connectivity for businesses and the workplace. Unlike 5G technologies, Wi-Fi operates in unlicensed spectrum bands. In the coming years, 5G and Wi-Fi 6 will co-exist to support different use cases, namely, Wi-Fi 6 works better for indoor networks, such as office spaces, and 5G works better for outdoor networks such as connecting users to the network while in transit. Coupled with new and emerging wireless network technologies, enterprises and Federal agencies will require similar changes to their existing wired networks. Wired connections enable increased security, control, reliability, and speed over wireless alternatives. Wired connections provide users more dedicated bandwidth, less network traffic interruptions, and less susceptibility to interference and outages. The most obvious drawback of wired connections is that it inhibits workforce mobility and requires collaboration with facilities management to maintain workplace organization and cable management.[28]

Ethernet and Fiber Connectivity

Federal agencies will continue to maintain both wireless and wired network connections in the near future. Although new 5G and Wi-Fi 6 will enable super fast wireless applications, data transfer speeds are limited by the radio frequency spectrum, which can also lead to interference. Agencies will continue to invest in wired connection to ensure their staff can effectively execute agency missions. Underneath all wireless networks lies wired cables, typically either fiber or copper cabling. Copper cabling, such as Ethernet, is cheaper and is becoming faster, but has distance limitations and is prone to interference. Fiber has faster speeds, greater security, and more reliable data delivery over long distances, but is more expensive than copper alternatives.[29]

Ethernet cabling continues to improve and newer categories can support higher performance. Next generation Ethernet versions Cat6 and Cat6a are faster than Cat5e predecessors and can support up to 10 Gbps. Cat7 wiring can potentially transmit up to 40 Gbps at 50 meters and even 100 Gbps at 15 meters is currently under development. While Cat6 and Cat6a wiring offer higher performance rates than previous versions, many LANs still opt for Cat5e due to its cost-effectiveness and ability to support Gigabit speeds. For most agencies, Cat5e cabling will suffice for normal business operations. Additionally, Cat6 and Cat6a cables are thicker than the Cat5e cables and upgrading may require physical changes to existing facilities. Agencies should assess the business case for upgrading their wired physical network infrastructure. For many agencies, existing Cat5e provides sufficient speed and reliability to perform normal business functions.[30]

Software Defined Networking

[28] Wired Vs Wireless In Business: Why You Should Still Wire Up Your Office For Data. 02 May 2018. https://www.altitudeintegrations.com/wired-vs-wireless-in-business-why-you-should-still-wire-up-your-office-for-data/

[29] Mailheau, Rita. The Cable War: Copper vs. Fiber. 30 June 2017. https://www.versatek.com/blog/cable-war-copper-vs-fiber/

[30] From conversations with Network and Telecommunications SMEs at GSA on 20 May 2019.

Traditional networks used integrated hardware and software to direct traffic across a series of routers and switches. In recent years, the explosion of mobile devices and edge computing, server virtualization, and the increased use of cloud computing have brought about changes to traditional network management. Software Defined Networking (SDN) simplifies network management by allowing network managers to centrally configure routers and switches using software applications, instead of having to individually configure routers and switches. By centralizing network state in the control layer, SDN gives network managers the flexibility to configure, manage, secure, and optimize network resources via dynamic, automated SDN programs, and therefore, respond quickly to changing business requirements. Moreover, they can write these programs themselves and not wait for features to be embedded in vendors' proprietary and closed software environments.

Additionally, the rise of SDN has paved the way for increased security controls and microsegementation of the network. Traditional firewalls, access control lists (ACLs), and intrusion prevention systems (IPS) are designed to inspect and secure network traffic coming into the data center. Microsegmentation gives businesses and agencies greater control over the lateral communication that occurs between servers, and therefore, is unaffected by perimeter-based security tools. If a breach occurs, microsegmentation can limit the lateral intrusion of networks by hackers. Microsegmentation allows network managers and security teams to tailor security settings to different types of traffic and create policies that limit network traffic. By applying these rules and policies, network managers decrease the network attack surface and can limit the impact and disruption to the business caused by intrusion. Although microsegmentation has several benefits, it still requires that businesses and agencies have visibility into application connections and dependencies, which remains a challenge for some agencies.

Software Defined Wide Area Networking (SD-WAN)

Software Defined Wide-Area Networking (SD-WAN) provides software defined application routing to the wide area network (WAN), which connects an organization's many separate locations. Traditionally, corporate networks that connect multiple locations were based around centralized control, routing, and security with all network traffic being routed through a main data center. That model is changing with many businesses and agencies running applications in the cloud and with many end users connecting to the network through the open Internet on their mobile devices. For these reasons, many businesses and agencies are moving to SD-WAN. SD-WAN allows networks to route traffic based on centrally-managed roles and rules, independent of the entry and exit points of the traffic. Ultimately, SD-WAN will make it easier for machine intelligence to take a hand in network management, further lowering bandwidth expenses and improving security.[31] SD-WAN provides software-defined application routing to the WAN and connecting enterprise networks over large geographic distances.

Despite the growth of SDN and SD-WAN, many businesses and agencies continue to rely on Multiprotocol Label Switching (MPLS), which is likely to remain in use in the near future. MPLS is a packet-forwarding technique that uses labels in order to make predetermined data routing decisions between two or more locations. Although MPLS is not as modern as SD-WAN, it does offer some advantages such as increased reliability of packet delivery, avoidance of packet loss, and traffic predictability. One critical factor is that SD-WAN requires a much higher level skill set to manage network traffic than MPLS. Some analysts argue that federal agencies will struggle to have the staff in place to

[31] Oswal, Anand. The 5 Technologies that will Change Networking in 2019. 08 Jan 2019. https://blogs.cisco.com/enterprise/the-5-technologies-that-will-change-networking-in-2019

manage and secure SD-WAN and will have to outsource these roles to contractor and vendor communities. Agencies should prioritize upskilling network managers in order implement SD-WAN in their organizations.[32]

Intent-Based Networking (IBN)

Intent-Based Networking (IBN) is a rapidly emerging new technology for automating the management of highly complex networks.[33] IBN solutions are software that provide life cycle management for networking infrastructure and automatically plan, design, and implement network changes.[34] This is accomplished by deploying Machine Learning (ML) and Network Orchestration (NO) tools to align high-level business and application requirements across the entire networks without the need for traditional manual network configuration techniques, which tend to be manually implemented, time consuming, and mistake prone.[35] IBN promises a paradigm shift where network users and operators manage their operations by stating high-level "intents" that are then translated and automatically executed by software algorithms, thus greatly increasing the simplicity, agility, and programmability of complex networks.

SDN and IBN are complementary technologies likely to fundamentally change the way networks are operated and managed. SDN automates and virtualizes physical network devices and IBN focuses on aligning network infrastructure to high-level business goals and maintaining and improving that alignment over time.[36] While SDN is deployed in the field today, IBN is still emerging and will benefit from improvements in AI and ML algorithms. Furthermore, many enterprises, and especially Federal agencies, have large inventories of legacy network equipment and systems, which will present a major challenge to deploying IBN effectively.[37] Gartner estimates that IBN products will not be commercially available until 2020.[38] Overall, IBN is an emerging technology that will likely upend traditional network management and operations for enterprises and Federal agencies in the future.

Considerations for CIOs

Enterprise Infrastructure Solutions (EIS) Contract

The Enterprise Infrastructure Solutions (EIS) is a competitive multiple award indefinite delivery/indefinite quantity (IDIQ) contract that will allow federal agencies to buy network and telecommunications products and services over the next 15 years. The EIS contract has a 5-year base period with two 5-year options

[32] From conversations with Network and Telecommunications SMEs at GSA on 20 May 2019.
[33] Kinghorn, Gary. Intent-based Networking. Is it real? Are you ready? Brighttalk webcast. 26 June 2018. https://www.brighttalk.com/webcast/16297/324037/intent-based-networking-is-it-real-are-you-ready
[34] Lerner, Andrew. Intent-based Networking. 07 Feb 2017. https://blogs.gartner.com/andrew-lerner/2017/02/07/intent-based-networking/
[35] Veriflow. Intent-Based Networking: Top 10 Questions and Answers. https://www.veriflow.net/_downloads/Intent-based%20Top%20questions.pdf
[36] Ibid.
[37] Saha et al. Intent-Based Networks: An Industrial Perspective. Oct 2018. https://www.researchgate.net/publication/328242908_Intent-based_Networks_An_Industrial_Perspective
[38] Skorupa, Joe, Andrew Lerner, and Sanjit Ganguli. Gartner Research. Innovation Insight: Intent-Based Networking Systems. 07 Feb 2017. https://www.gartner.com/en/documents/3599617/innovation-insight-intent-based-networking-systems

and a ceiling value of $50 billion.[39] EIS consolidates up to 93 separate existing contract vehicles from the current Networx Universal contracts, Washington Interagency Telecommunications System (WITS) 3, and GSA Regional Local Service Agreement (LSA) contract vehicles and simplifies the process of acquiring telecommunications and IT products and services. GSA negotiated the extension of the Networx contracts until March 2020 and the WITS3 and 65 Regional LSA contracts until May 2020. In December of 2018, GSA agreed to extend existing telecommunications contracts to 2023 to provide agencies with additional time to transition and modernize.[40] GSA has previously stated that the EIS contract will provide agencies the flexibility needed to maintain services in-line with evolving standards for emerging network technologies and security requirements.

The Policy Ecosystem

On June 24, 2019, OMB released Cloud Smart, the first update to the federal cloud strategy since Cloud First was published in 2010. Cloud Smart provides practical implementation guidance for agencies and emphasizes security, procurement, and workforce development for successful cloud adoption and IT modernization.[41] The new federal cloud strategy calls for critical OMB policies, many of which affect agency network modernization efforts, including the Data Center Optimization Initiative (DCOI), Trusted Internet Connection (TIC) policy, Identity, Credential, and Access Management (ICAM) policy, and the Continuous Diagnostics and Mitigation (CDM) program, to be updated to meet agency needs and emerging technology requirements. The following list of relevant policies are critical to ensuring the security of existing network architectures.

Continuous Diagnostics and Mitigation (CDM)
The CDM Program enhances the overall security posture of the Federal Government by providing Federal agencies with capabilities to monitor vulnerabilities and threats to their networks in near real-time.[42] The key objectives of the CDM Program are to reduce agency threat surface, streamline Federal Information Security Modernization Act (FISMA) reporting, increase visibility into federal cybersecurity, and improve the ability to respond to federal cybersecurity issues.[43]

Data Center Optimization Initiative (DCOI)
The Office of Management and Budget (OMB) released updated the Data Center Optimization Initiative (DCOI) policy on June 25, 2019 to require the consolidation and optimization of data centers. Furthermore, the new DCOI policy identifies agencies' Key Mission Facilities (KMFs), many which have unique network bandwidth or security requirements, such as special-purpose processing nodes (SPPNs) or high performance computing (HPC) systems.

---

[39] General Services Administration. Telecommunications and Network Services. Enterprise Infrastructure Solutions. https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-infrastructure-solutions

[40] General Services Administration. Telecommunications and Network Services. Enterprise Infrastructure Solutions. https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-infrastructure-solutions/enterprise-infrastructure-solutions-contract-basics

[41] Federal Cloud Computing Strategy. https://cloud.cio.gov/strategy/

[42] M-19-02. Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements. https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf

[43] General Services Administration. Telecommunications and Network Services. Continuous Diagnostics & Mitigation (CDM) Program. https://www.gsa.gov/technology/technology-products-services/it-security/continuous-diagnostics-mitigation-cdm-program

Identity, Credential, and Access Management (ICAM)

With the rise of cloud and mobile computing, there is increased traffic of federally-owned data from internal networks to external users.[44] Updated ICAM policy was released by OMB in May 2019, which encourages agencies to use more flexible solution for identity and access management, supports authentication pilot programs, and require agencies to create dedicated ICAM teams.[45]

Internet Protocol Version 6 (IPv6)

All devices that connect to the internet have an Internet protocol (IP) address. The increase in Internet users and devices in recent years led to the exhaustion of available IPv4 addresses. IPv6 ensures the availability of new IP addresses in the future.[46] OMB is in the process of finalizing policy related to the transition to IPv6. To realize the technical, economic, and security benefits of operating a single, modern, and scalable network architecture, the new policy communicates to agencies the need to "complete the operational IPv6 deployment across all Federal information systems and services, and to enable and encourage agencies to migrate to IPv6-only systems" as well as phase out the use of IPv4 systems[47]

Trusted Internet Connections (TIC) Initiative

The purpose of the Trusted Internet Connection (TIC) initiative is to enhance network security by reducing the number of Internet gateways on Federal Government networks and ensuring all external connections are routed through designated TICs.[48] On December 14, 2018, OMB released draft updated TIC Initiative policy that directs the Department of Homeland Security (DHS) to create a set of use cases for how agencies can establish safe internet connections for cloud services, agency branch offices, and remote users without having to route network traffic through a prescribed set of physical access points.[49]

Zero Trust (ZT) Architecture

Given the distributed nature of cloud and the growing number of mobile users, agencies should move security and controls from the perimeter of their networks to the data layer in order to ensure data security.[50] Zero Trust (ZT) is a security approach that starts with the assumption that the network is inherently hostile and that internal and external threats exist at all times, and therefore, all devices, users, and traffic must be continuously authenticated and authorized in an automated and unburdensome manner.[51] Multiple agencies are currently piloting ZT architectures, including DOD and NASA.

Zero Trust Use Case

The National Security Agency (NSA) and the Defense Information Systems Agency (DISA) are collaborating on a ZT pilot within the Department of Defense (DOD). The pilot program aims to incorporate about 2,200 endpoint users into a ZT framework by the end of calendar year 2019, with plans to scale the program in future phases. To date, the pilot has successfully demonstrated the increased security posture of ZT and DOD is moving faster than other government agencies in proving

[44] M-17-19. Enabling Mission Delivery through Improved Identity, Credential, and Access Management. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[45] M-17-19. Enabling Mission Delivery through Improved Identity, Credential, and Access Management. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[46] Federal Communications Commission. Internet Protocol Version 6: IPv6 for Consumers. https://www.fcc.gov/consumers/guides/internet-protocol-version-6-ipv6-consumers
[47] Draft OMB Policy Memo. Completing the Transition to Internet Protocol Version 6 (IPv6)
[48] M-08-05. Implementation of Trusted Internet Connections (TIC). https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf
[49] Draft Policy. Update to the Trusted Internet Connection (TIC) Initiative. https://policy.cio.gov/tic-draft/
[50] Federal Cloud Computing Strategy. https://cloud.cio.gov/strategy/
[51] Ibid.

ZT as a scalable security model. Many senior leaders within Cyber Command and DISA believe ZT is the future of DOD networks. Agencies are encouraged to connect with and learn from DISA and others within DOD leading efforts to implement ZT.

The ICAM and CDM function as prerequisites for comprehensive ZT. Being able to identify who is accessing the network is critical to verifying trust and granting access in a Zero Trust architecture. Furthermore, Zero Trust can help overcome some of the hardware vendor challenges, such as the acquisition restrictions on foreign hardware manufacturers, by assuming all systems and hardware are untrustworthy.

Suggested Actions for Agencies

This white paper informs CIOs across government of the emerging technologies likely to affect their network architectures in the near future. In addition to level setting, this white paper provides several suggested actions agencies can incorporate into existing network modernization strategies.

1. Survey the Technology Landscape

Many of the emerging technologies discussed in this white paper, such as 5G, SD-WAN, and next generation fiber and Ethernet cabling have the potential to disrupt how agencies manage their networks. CIOs in government should work to ensure broad awareness of new networking trends and technologies throughout their agencies. This can be accomplished by socializing resources such as this white paper and the resources cited herein.

2. Incorporate Pilots and Knowledge Sharing into Existing Strategies

As part of agencies' network modernization strategies, CIOs should assess the applicability and business case for emerging networking technologies. For technologies that will enhance or enable mission delivery, agencies should conduct pilots of their own, incorporating lessons learned from other pilots throughout government, and create roadmaps for future scaling and agency-wide implementation.

3. Upskilling and Continuous Learning for Network Managers

Managing agency networks using SD-WAN requires a higher level skill set than managing traditional network configurations. In order to realize the benefits of these new technologies, CIOs should include network manager upskilling into their strategies.

4. Collaborate with GSA on Acquisition Milestones and Best Practices

Agency network modernization strategies should incorporate EIS milestones. Many of the emerging network technologies discussed in this white paper, such as 5G services and infrastructure, are covered by the EIS contract. Furthermore, GSA has produced and continues to develop implementation guidance for agencies, such as the 5G implementation white paper[52] and EIS Transition Full Service Transition Plan.[53]

[52] Zielinski, Bill. Way Beyond Wireless: Planning for 5G. 30 July 2019. https://gsablogs.gsa.gov/technology/2019/07/30/way-beyond-wireless-planning-for-5g/

[53] Enterprise Infrastructure Solutions (EIS) GSA Assisted Transition (GSAAT) Full Service Transition Plan Version 5.0. https://www.gsa.gov/cdnstatic/GSA_TCC_Full_Service_Transition_Plan_v5_041819.pdf

Acknowledgements

This White Paper was produced by the CIO Council's Innovation Committee and would not have been possible without contributions from the Office of Management and Budget's Office of the Federal Chief Information Officer, the General Services Administration's Office of Government-wide Policy, and support from REI Systems, Inc. and Incapsulate, LLC.

Originally established by Executive Order 13011 (Federal Information Technology) and later codified by the E-Government Act of 2002, the CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources.

The CIO Council is one element of an interagency support structure established to achieve information resource management objectives delineated in legislation including the E-Government Act of 2002, Government Paperwork Elimination Act, Paperwork Reduction Act, Government Performance and Results Act, and the Information Technology Management Reform Act of 1996.

FOR MORE INFORMATION

Contact email@cio.gov
visit www.cio.gov