MODERNIZING FEDERAL AGENCY IT AND SECURITY WITH GSA'S ENTERPRISE INFRASTRUCTURE SOLUTIONS (EIS) CONTRACT

EXECUTIVE SUMMARY

The General Services Administration's (GSA's) $50 billion Enterprise Infrastructure Solutions (EIS) contract is a perfect opportunity for federal agencies to modernize their network infrastructures by embracing new architectural approaches, including software-defined networking (SDN), a cloud-based model for Trusted Internet Connections (TIC), protection for high-value assets, network segmentation, and zero trust network enablement.

More than three years ago, GSA identified May 2020 as the target date for completing the transition to EIS. With more than half of that time window now elapsed and security risks increasing every day, agencies should act now to begin the modernization process.

Cybersecurity improvement is a major goal of the GSA EIS contract.

Federal officials see EIS as a way to help small agencies.

WHITE PAPER

FOR FEDERAL AGENCIES, CYBERSECURITY IS JOB ONE

Cybersecurity threats are rapidly transforming, and cyber adversaries are constantly refining their tools and techniques. By contrast, federal agencies' security postures tend to be less agile. Many agencies use an assortment of security solutions that fail to share information, which leaves them exposed to emerging and advanced threats. Most federal agencies need to improve their threat detection and remediation capabilities, address security gaps, and replace solutions that aren't best of breed with new technologies that are constantly being developed and refined to counter ever-changing cyber threats.

The EIS contract is designed to help them do just that. It leverages the bulk purchasing power of the federal government to help agencies improve their telecommunications and network infrastructure and adopt more modern networking technologies, including SDN and 5G wireless networks. EIS replaces GSA's Networx Universal and Enterprise contract as well as GSA Regional Local Service Agreements for government telecommunications and infrastructure solutions. With a 15-year period of performance, the EIS contract is valued at $50 billion.

EIS also gives smaller agencies an opportunity to catch up, as they face unique challenges and typically lag behind larger agencies in cybersecurity capabilities, making them more vulnerable to attacks. An August 2017 report to the president on federal IT modernization suggested EIS can help smaller agencies manage their information security programs.[1] EIS gives agencies the flexibility to choose security tools "a la carte," as well as opportunities to consolidate the acquisition of managed security services with other small agencies.

Federal government agencies face an increasing number of data breaches.

57% of government IT leaders reported a data breach in 2017.

That's up from just 34% in 2016.[2]

SECURITY MODERNIZATION CHALLENGES

It's no wonder that Tony Scott, former federal CIO, called outdated federal IT systems "a crisis that is bigger than Y2K."[3] In addition to the staggering cost differential between maintaining legacy systems versus new technology, many federal agencies' security isn't as strong as it could be, and as a result there have been many serious data breaches in recent years.

EIS should help agencies choose security services "a la carte."

OUTDATED IT EQUIPMENT—SOME DECADES OLD

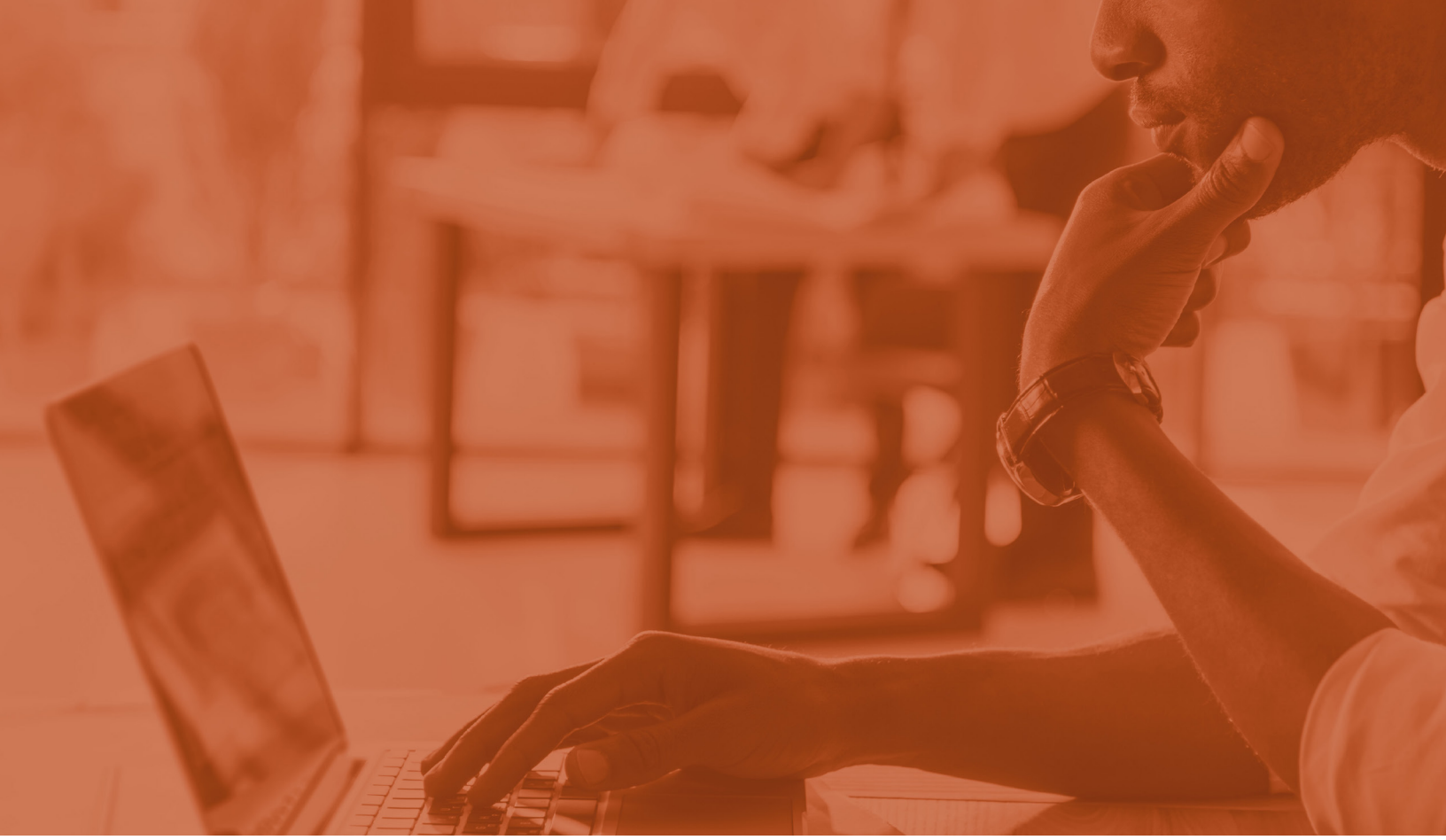
It's no secret to hackers that government security solutions or technology are largely out of date. As late as May 2016, the U.S. Department of Defense was running an important nuclear communications network, used to issue launch orders, on computers using floppy disks.[4]

Agency systems, some more than two decades old, are not only vulnerable to cyberattacks but also expensive to maintain. About three-quarters of the $80 billion the U.S. government budgets for IT each year is spent maintaining legacy systems.[5] Transitioning to the EIS contract enables agencies to not just modernize their transport and access options but also modernize the equipment that supports this connectivity and the technology that secures the data.

DISPARATE SECURITY PRODUCTS

When security products are added on to a network to address a new requirement, but those products don't integrate with the network's legacy security solutions, the "update" often creates more problems than it solves. Additionally, many agencies are now living with the results that include:

- Inability to automatically respond to threats: Products that aren't integrated can't share threat intelligence, so they can't all respond quickly whenever one security solution on the network detects a threat.
- Security gaps: It's difficult to pinpoint security gaps when there is no centralized visibility across the network's entire attack surface. This lack of visibility not only diminishes the security posture of the agency, but because the agency may not understand its risks, it also inhibits the ability of IT leaders to deploy the right telecom and security solutions to address remaining vulnerabilities.



Federal agencies' hodgepodge security infrastructure limits their willingness to consider new security tools for other reasons as well. New security products may not integrate with their existing systems, and they may require long deployment cycles before agencies can take advantage of them. New technologies can enable the consolidation of capabilities such as routing and security policy enforcement into fewer devices, simplifying the network.

Running a plethora of disparate security products also presents IT management challenges, as diverse systems require more staff, with specific security skill sets, to manage. Like the private sector, federal agencies face an ongoing cybersecurity skills shortage, making this a difficult problem to solve.

OPPORTUNITIES AND RESPONSIBILITIES FOR AGENCY LEADERS

Federal government agency leaders responsible for managing requirements and contracts with the prime contractors managing EIS should ask questions about what new capabilities will be offered, how contracts will be administered and future-proofed, and how payments can be structured to migrate seamlessly to the new EIS model. Federal agencies can use this opportunity to replace older, more expensive technology. For example, they might replace T1 lines with alternative methods of network access such as satellite, cable, and wireless, and simultaneously deploy advanced technology to secure the new solutions, to drive down costs over time and simplify their networks.

Currently, there are nine prime contractors (most, but not all, telecom carriers) administering EIS. All must transition to new agency contracts by 2020, making it critical for agencies to begin the modernization process as soon as possible. By offering a security fabric that enables transparent visibility and control across the agencies' attack surface, carriers have the opportunity to offer new services such as analytics and risk management.

The prime contractors are in a unique position to transform federal agencies into hybrid environments and eventually into their desired state. For example, an agency that envisions a software-defined wide-area network (SD-WAN) infrastructure but is running multiprotocol label switching (MPLS) today could turn to an EIS prime contractor to enable both technologies and transition entirely to SD-WAN over time. Additionally, universal CPE products with virtual product instances deployed at each site can enable easier turnup/teardown of features and avoid truck rolls.

Agencies should choose carriers that are actively modernizing their existing infrastructure and working closely with security vendors to offer new capabilities. Make sure your EIS partner has security on the forefront and can offer the following:

- Built-in compliance updates, tracking, and reporting
- Automated vulnerability and patch updates
- Streamlined intrusion and breach detection and remediation to minimize the impact of threats and attacks

- Segmentation across users, networks, and applications, allowing agencies to thwart intrusions and minimize the depth and breadth of breaches
- Simplifed security deployment and management by integrating security and network capabilities and automating manual tasks

CONCLUSION

By modernizing their security posture with the capabilities described in this white paper, agencies can address modern risks such as targeted phishing campaigns, ransomware, insider threats, and weaponized artificial intelligence (AI). In fact, agencies should not even attempt network and infrastrucuture modernization without considering the most advanced security architecture and tools. Modern security solutions can also help agencies comply—and demonstrate their compliance—with regulations such as the Federal Information Security Management Act (FISMA), which requires agencies to develop and document their information security programs.

With major security risks surfacing every day, it's critical for agencies to get the most out of the EIS contract and gain access to new tools to fight data breaches and other cybersecurity risks.

RECENT FEDERAL GOVERNMENT DATA BREACHES

- In June 2015, the U.S. Office of Personnel Management (OPM) announced a breach affecting 21.5 million records. The two breaches, from 2014, affected government workers and other people who had undergone background checks. OPM's director and CIO both resigned after the incident.[6]
- In April 2017, the Internal Revenue Service (IRS) revealed that up to 100,000 taxpayers may have had their personal information compromised because of a vulnerability in the IRS Data Retrieval Tool, which is used to complete the Free Application for Federal Student Aid. The cost to the agency was reportedly about $30 million.[7]
- In September, the U.S. Securities and Exchange Commission (SEC) reported a 2016 data breach that the SEC had originally believed had a limited impact. However, in 2017, the SEC discovered that the software vulnerability in its EDGAR system "… may have provided the basis for illicit gain through trading."[8]

[1] "Report to the President on Federal IT Modernization," itmodernization.cio.gov, accessed June 22, 2018.

[2] Scharon Harding, "U.S. federal government data breaches saw 'huge' increase in 2017," Channelnomics.com, February 22, 2018.

[3] Phil Goldstein, "Legacy Federal IT Systems Are a Ticking Time Bomb of Risks," FedTech, December 7, 2015.

[4] Brian Fung, "The real reason America controls its nukes with ancient floppy disks," The Washington Post, May 26, 2016.

[5] Zack Whittaker, "US government is spending billions on old tech that barely works, says watchdog," ZDNet.com, May 25, 2016.

[6] Aaron Boyd, "OPM CIO Seymour resigns days before Oversight hearing," Federal Times, February 22, 2016.

[7] Alfred Ng, "Hackers use college student loans tool to steal $30 million," CNet.com, April 7, 2017.

[8] "SEC Chairman Clayton Issues Statement on Cybersecurity," SEC.gov, September 20, 2017.

September11,201810:43AM

186576-0-0-EN

WP-EIS-problem-education-2