Your Guide to Key Advancements in Government Cybersecurity
CenturyLink Network Security

Securing Government IT Today for a Better Tomorrow

Cyberthreats are persistent and stealthy. CenturyLink tracks nearly 200,000 threats per day that impact over 100 million unique targets.¹ We help agencies and organizations proactively thwart threats before they become security breaches.

Benefits of the CenturyLink Security Portfolio:

- Managed Security Services, E3A, ECS, MTIPS, DDOS, NBS(ANS), CDM
- Limit exposure to cyberattacks with multi-layered security services
- Comply with government cybersecurity and connectivity policies
- Identify cyberthreats with threat intelligence, monitoring, detection and mitigation
- Analyze cyberattacks with analytics and threat management services

CenturyLink solutions are available on multiple, approved government contract vehicles including:

- Enterprise Infrastructure Solutions (EIS)
- General Services Administration (GSA) IT Schedule 70
- Networx Enterprise and Universal
- Alliant 2
- WITS 3
- Connections II, plus more

As a network provider, we are positioned to protect customer data before it gets to the customer premise.


Call 1.886.9FEDNET or visit centurylink.com/federal for contract information.
Enhancing Government Cybersecurity With Managed Services

An Interview with Dave Young, Vice President for Strategic Government, CenturyLink

There’s no shortage of policies, regulations and standards outlining how agencies should protect the government’s most critical systems and data.

In fact, over the past several years the Government Accountability Office (GAO) has made about 2,500 recommendations for federal agencies to enhance their information security programs and controls, according to a 2017 GAO report.

“The challenge seems to be execution,” David Young, Senior Vice President for Strategic Government at CenturyLink, said in a recent interview with GovLoop. “With that lens, you look at funding, staffing and training. There is a lot of work that needs to get done, so finding ways to speed that up is essential.”

As a major player in the critical infrastructure space, CenturyLink works closely with government agencies to lower their cybersecurity risks, improve compliance and protect their assets using flexible and cost-effective IT security solutions. But part of the challenge for companies and their government customers is trying to keep pace with constantly evolving cyberthreats while wading through regulatory hurdles. These impediments include burdensome acquisition and operational compliance requirements that slow the adoption of critical cyber capabilities, Young said.

Young highlighted two Homeland Security Department programs that are enabling agencies to target malicious cyberthreats. Under the Einstein 3 Accelerated (E3A) program, CenturyLink is one of few approved internet service providers that supports near real-time inspection of federal network traffic and then blocks any known or suspected cyberthreats.

Through DHS’s Enhanced Cybersecurity Service (ECS) program, CenturyLink uses threat indicators provided by the government to augment critical infrastructure companies’ existing capabilities. Specifically, this managed service offering allows owners and operators of critical infrastructure to block access to specific malicious domain names and stop emails with specific malicious criteria from entering a network.

Such programs are vital for agencies and critical infrastructure operators considering that most email antivirus programs catch, on average, only 45 percent of cyber criminal activity, leaving organizations open to risks like phishing, bots and other social media engineering techniques.

“Our security portfolio provides layers of enhanced cybersecurity protections to protect customer data from computers to the cloud,” Young said.

But agencies should not be satisfied with simply checking a box to meet security requirements. They must constantly examine changing cyberthreats and work with their internal and external partners to respond accordingly.

In terms of capacity and the demand that cybersecurity puts on the workforce, having access to managed services like those offered by CenturyLink provides agencies with cyber capabilities that are immediately operational and cost-effective, especially for smaller agencies, Young said.

“Cyberthreats adapt very quickly, and keeping pace is hard enough,” Young said. “That’s why more communication is necessary.”

Partnerships, such as participating in the President’s National Security Telecommunications Advisory Committee (NSTAC), are one example of how the public sector is working closely with the private sector, including CenturyLink, to share important insights that can improve the availability and reliability of telecommunication services.

CenturyLink also has its own threat lab, which was designed to provide customers with consumable information that gives organizations increased situational awareness and helps them align their cyber capabilities with active threats around the world.

In addition to improved information sharing, there are promising solutions that agencies should have on their radar as cybersecurity continues to evolve. But as with any new capability, it takes time for these technologies to mature.

“For example, network function virtualization is a great way to deliver capabilities in the network, where they are consumed,” Young said. “Because of the inherent virtualization and the decoupling of capability from hardware, there is a quicker turnaround time for delivering the capabilities that our customers want and demand.”

The key for agencies is finding the right balance that enables them to meet rigorous federal standards while still having the flexibility to quickly adapt to cyberthreats.

“Anything that impedes the loop from capability to deployment needs to be examined very carefully,” Young said. Once agencies identify and remove these barriers, they can focus their time and resources on adopting capabilities that meet their most pressing cyber needs.