GAIN AN INSIDER'S VIEW OF HOMELAND SECURITY DEPARTMENT THREAT INTELLIGENCE

By CyberScoop Staff

At no other time in history has the nation's critical infrastructure — the facilities, services and institutions upon which our way of life depends — faced a broader array of threats. From sophisticated cyberattacks to natural and manmade disasters, the companies and government agencies responsible for operating and protecting our critical infrastructures are under constant assault.

"Russia, China, Iran, and North Korea … have probed American critical infrastructure, with varying degrees of sophistication and success," said James A. Lewis, senior vice president at the Center for Strategic and International Studies, during a Senate Judiciary Committee hearing on Aug. 21. "The most important critical infrastructures are energy, finance, telecommunications and government services," he said. "None of these are secure if Russia, Iran, or other states chose to attack them."

Lewis' warning may sound extreme, but the size, scope, complexity and interconnectedness of the nation's critical infrastructure sectors — there are 16, according to the Department of Homeland Security — put them beyond the ability of the federal government to defend alone.

That's why DHS has been working directly with a handful of select internet and telecom providers to offer Enhanced Cybersecurity Services (ECS) to private-sector critical infrastructure operators, as well as companies based in the U.S. in general. The DHS-authorized services take advantage of the government's "secret sauce," which identifies threat signatures, network traffic patterns and other technical indicators that show hackers at work on a system.

For CEOs and executive teams responsible for safeguarding critical infrastructure facilities, ECS providers represent an increasingly potent resource for combatting cyberthreats.

Insider perspective

CenturyLink, for example, has offered Enhanced Cybersecurity Services since the program's inception in 2010. A significant portion of the world's internet traffic moves across CenturyLink's network every day. That gives CenturyLink a powerful advantage in offering critical infrastructure providers as well as private sector companies a deep expertise in stopping malicious attacks.

CenturyLink's expertise as a global ISP has placed the company in key roles within DHS's National Cybersecurity and Communications Integration Center (NCCIC) and Communications Information Sharing and Analysis Center (ISAC). This relationship with DHS also puts the company in a unique position to help critical infrastructure providers leverage intrusion and detection services available via ECS, according to Dave Young, CenturyLink's senior vice president of strategic government.

"DHS works with agencies across the federal government to gather a broad range of sensitive cyberthreat information," Young said. "DHS then supplies those detailed cyberthreat indicators to CenturyLink, which integrates that data with its own threat indicators to help protect organizations from cyberattacks."

By incorporating these government-furnished threat indicators with its own threat intelligence, based on the traffic moving across its networks, "CenturyLink can provide ECS customers with network-based, inbound security measures that neutralize dangerous threats and prevent harmful code from becoming embedded into an organization's IT infrastructure," Young said.

Unique position

The company's ECS offering is no small accomplishment. It is one of only three communications service providers (CSPs) accredited and authorized by DHS to offer it.

CenturyLink provides similar enhanced security protections to hundreds of thousands of federal civilian end-users under the DHS Einstein 3 Accelerated (E3A) program. The E3A program detects malicious traffic targeting federal government networks and prevents that traffic from harming those networks.

The company's E3A offering is available to federal civilian agencies via DHS. CenturyLink's ECS capabilities are available to state and local governments and private critical-infrastructure companies, even if they don't get their connectivity from CenturyLink. ECS has been available on the company's GSA Schedule 70 procurement contract vehicle since 2016.

"DHS collects a lot of threat information, and that's what we can provide to critical infrastructure operators," said Young. "They can't get that information directly from DHS. They can only get it through a communications service provider. And you have to be an ECS provider authorized by DHS."

Expanded visibility and security

CenturyLink also bolstered its position as one of the leading global communications providers with its $34 billion acquisition of Level 3 Communications in 2017. The merger added 200,000 miles to CenturyLink's network, which now connects more than 350 metropolitan areas. More importantly, the deal significantly enhanced CenturyLink's cybersecurity portfolio.

The integration of the two companies' networks means CenturyLink now monitors more than 114 billion NetFlow sessions and 1.3 billion security events per day, responding to and mitigating roughly 120 distributed denial-of-service (DDoS) attacks per day, according to company officials. This heightened visibility enables customers to better anticipate and protect against cyberthreats.

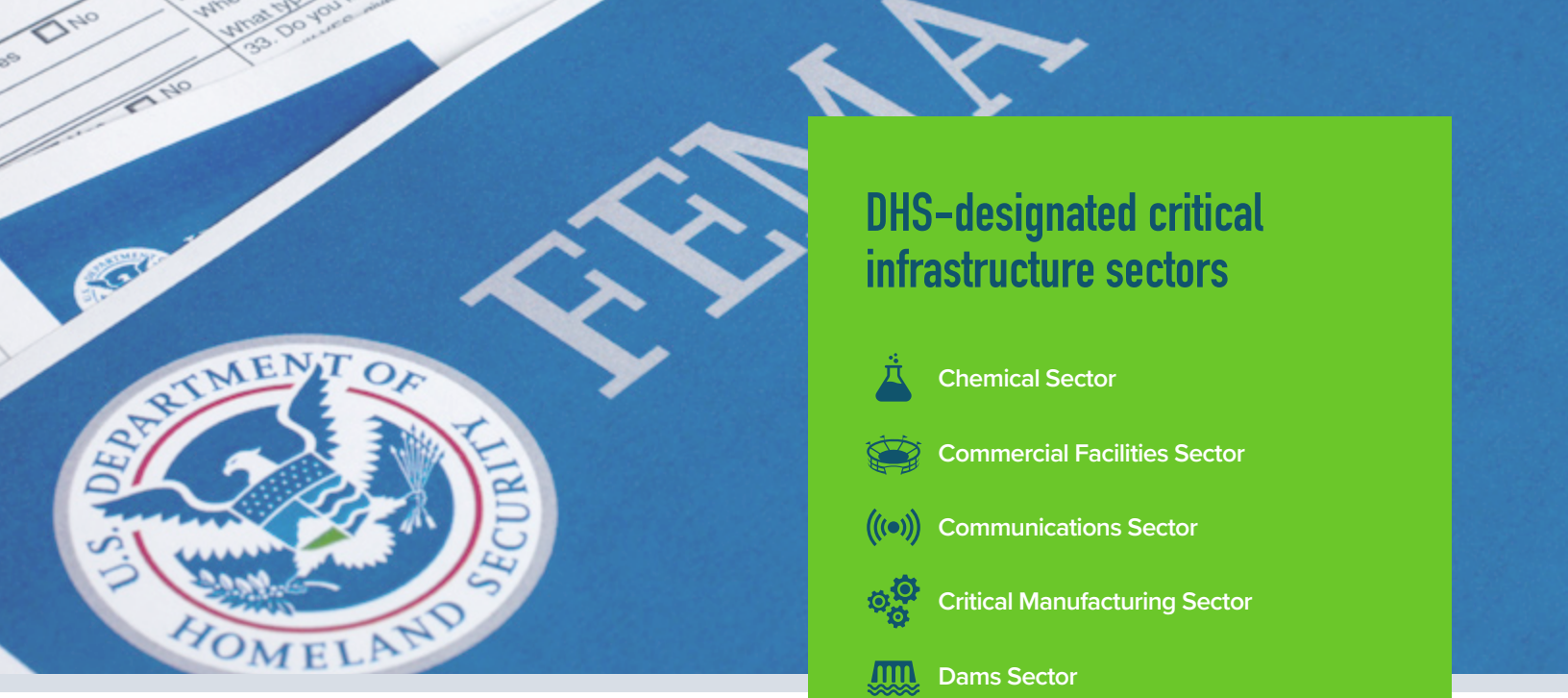
This enhanced threat awareness feeds into the company's comprehensive portfolio of security services, including Adaptive Threat Intelligence, a cloud-based capability that offers enterprise customers customized threat intelligence backed by CenturyLink's global IP backbone.

Adaptive Threat Intelligence also provides the ability to identify traffic originating from anonymous proxy networks, as well as improved threat scoring, fidelity and classifications for web hosting and Content Delivery Network providers associated with potentially malicious IP addresses. These features provide enterprises with actionable insight to bolster their cyber defenses.

> *"DHS collects a lot of threat information, and that's what we can provide to critical infrastructure operators. They can't get that information directly from DHS. They can only get it through a communications service provider. And you have to be an ECS provider authorized by DHS."*

–Dave Young
SVP of Strategic Government, CenturyLink

Combined with CenturyLink's strategic relationship with DHS, its global view of daily network traffic activity, these managed security services and Adaptive Threat Intelligence capabilities offer a distinct advantage to critical infrastructure operators and risk-minded corporate executives who find themselves increasingly having to defend against sophisticated, nation-state sponsored cyberattacks.



Support for critical infrastructure and key resources sectors

As a leading global communications service provider, CenturyLink plays a significant role during national emergencies.

"The government relies on CenturyLink to collaborate with them during times of emergency to provide continuous service," said Dave Young, CenturyLink's senior vice president of strategic government. "We go in and train FEMA how they should respond to disasters, how to prioritize re-establishing communications after wildfires and hurricanes, running exercises and drills," he said. "It's part of our DNA."

But the company's day-to-day visibility of global network activity and its expertise as a DHS-authorized Enhanced Cybersecurity Services provider allows CenturyLink to provide expert advice to the nation's critical infrastructure sectors as well as to private sectors companies.

***Learn more** about how CenturyLink's Enhanced Cybersecurity Services capabilities can help give your critical infrastructure team a critical edge in combating cyberthreats.*

DHS-designated critical infrastructure sectors

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food & Agriculture Sector
- Government Facilities Sector
- Healthcare & Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, & Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Source: DHS.gov

This article was produced by cyberscoop for, and sponsored by, CenturyLink®