Testimony of

R. David Mahon
Vice President and Chief Security Officer
CenturyLink

before the

Committee on Appropriations
Subcommittee on Homeland Security
United States Senate

Investing in Cybersecurity: Understanding Risks and Building Capabilities for the Future

Wednesday, May 7

Chairwoman Landrieu, Ranking Member Coats and members of the Committee, thank you for the opportunity to testify today on an issue that is of critical importance to national security, the US economy and homeland security. CenturyLink appreciates the leadership role the Department of Homeland Security plays in facilitating the cybersecurity of the nation's critical infrastructure, with the oversight and guidance of this Committee. In today's testimony, I would like to cover three key areas where the fiscal year 2015 budget offers worthwhile opportunities to strengthen the nation's cyber defenses:

- Further improving the quality of public-private information sharing related to cybersecurity;
- Leveraging classified cyber threat information to protect critical infrastructure and the networks of federal, state and local governments through the Einstein 3Accelerated and Enhanced Cybersecurity Service programs; and
- Investing in our cybersecurity workforce.

CenturyLink was founded nearly 85 years ago as a small rural telephone company with just 75 paid subscribers and a manual switch in the front parlor of the Williams family home in Oak Ridge, Louisiana. Our recent and rapid evolution through acquisition and innovation to become an $18.3 billion communications, data and cloud company with 47,000 employees, 13 million customers, a Tier 1 Internet backbone, and 55 data centers around the world makes us a prime example of how technology and communications infrastructure are driving our economy.

Effective cybersecurity is now central to everything we do, not only as a provider, but also as a customer of others. That includes our residential and enterprise broadband service, the secure communications services we provide to the Department of Defense, US embassies and Federal Communications Commission, our cloud computing platforms, and the managed security services we provide to critical infrastructure owners.

As the company has grown, we've benefited from excellent state and local support, enabling us to cultivate talent in northern Louisiana and the many local markets we serve in almost every state. This includes developing partnerships with the University of Louisiana – Monroe (ULM), Louisiana Tech University, the Cyber Innovation Center in Bossier City and other institutions. In fact, we are nearing completion of a 250,000 square foot Technology Center of Excellence on our Monroe headquarters campus that will house an additional 800 innovation professionals devoted to network monitoring, research and development, as well as IT and engineering support to our international service footprint.

In addition to our company-specific cybersecurity and risk management programs, CenturyLink has had a productive experience participating in the public-private partnerships established to share information and work collaboratively on industry-wide security challenges. Our executives serve on the President's National Security Telecommunications Advisory Committee (NSTAC), the Communications Sector Coordinating Council (CSCC), the Communications Information Sharing and Analysis Center (ISAC), and the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), among others. Through these efforts, we supported DHS in the creation of the National Cybersecurity and Communications Integration Center (NCCIC) and CenturyLink maintains a permanent presence on the NCCIC floor.

We support the voluntary, industry-led approach to protecting the security of critical infrastructure networks operated by the private sector, and appreciate the work the National Institute of Standards and Technology (NIST) has undertaken to create the Cybersecurity Framework, as well as DHS's Critical Infrastructure Cyber Community (C^3) Voluntary Program to educate stakeholders and promote the framework's use. CenturyLink has found the Framework useful in affirming many of the practices that we and other larger carriers already had in place. We are also using the Framework as a tool to help our enterprise clients assess their own threat level and implement risk-based cybersecurity protections.

The Cybersecurity Threat and Information Sharing

If I could leave the Committee with one thought about cybersecurity risks, it is this: Don't limit your thinking to only addressing the issues of malware, viruses, denial of service attacks, social engineering, botnets or any of the other tactics used. Instead, think of cybersecurity in terms of the adversaries – the people on the other side of the computer, wherever they may be, who conceive and execute the breaches.

Especially where critical infrastructure is concerned, our adversaries are constantly studying their targets, probing networks, paying attention to the defenses we put up, and searching for the weakest link in the chain – even tracking federal efforts to promote security. Whether it's hacking the website of a technical conference so targeted employees will download malware when they register, or using the compromised systems of an HVAC contractor as an attack vector, they are adaptable. This makes the threat more formidable, but also offers a clue about how to build our cyber defenses.

As a general matter, CenturyLink's security team divides cyber threats into several key groups, each with varying levels of sophistication:

- Nation-state sponsored, which are often the most sophisticated, and generally motivated by economic and political espionage. Combating government-sponsored adversaries requires an advanced information security program. These data breaches can go completely undetected by the victim organization.
- Criminal activity, including organized crime. These attacks have a wide range of sophistication, and are generally focused on capturing information that can be monetized.
- Terrorism and sabotage. These are most concerned with doing damage, including physical damage, to the target entities.
- Hacktivism. Generally less sophisticated, these groups will use "soft targets" with less sophisticated information security practices to garner publicity and make their political points.
- Insider threats. These can be the toughest to guard against because they are "inside the perimeter" of the target itself.

Adversaries tend to cluster around an industry sector, based on the goals they want to achieve. For example, a criminal cartel that wants to exploit consumer credit card information will, perhaps, stand up a network of infected computers and launch a particular type of attack on point-of-sale systems across numerous retailers, using similar malware, attack vectors and tactics for covering their tracks. But a nation state that wants to exfiltrate confidential technical specs about a smartphone operating system will use a completely different strategy. Especially for the more sophisticated adversaries, the best long-run defense is to build closely coordinated defensive alliances around the targeted industries and our partners in government, and to study our adversaries as closely as they study us.

To draw an analogy, the cat-and-mouse nature of cybersecurity resembles offensive and defensive schemes in the National Football League. Every season, coaches devise new "attacks" to move the ball down the field, whether it's the old "west coast offense" or last year's "read option." If they're successful, defenses that rely on the comfort of understanding past, predictable plays won't be prepared to stop them, at least for a while. But the minute a new offensive scheme succeeds, every defensive coordinator in the league starts working on countermeasures to shut it down. And while the short-term countermeasure might be a zone blitz or a few tough hits on the quarterback, the long-term solution has everything to do with continually studying the game tapes and evolving the defense.

In the world of cybersecurity, we don't have the luxury of watching the "game" every Sunday, but the never-ending need to study the opposition and update defenses is the same. For

DHS and the nation's critical infrastructure providers, this means continuously refining the information sharing relationships to get actionable, tailored information to the targeted sectors in as close to real time as possible. This will ultimately lead to automating the information sharing mechanisms that will allow a targeted entity to use the cyber threat information to defend itself without compromising the sources and methods of the information provider. This is as much a cultural challenge as it is a technical one, because the information at issue is so sensitive and the teams are not accustomed to sharing their proverbial playbooks.

In our experience, the DHS leaders are fully aware of the challenge and committed to strengthening the partnerships, but doing so is often an iterative, painstaking process that involves continuously building trust, sophistication and technological capabilities, and we appreciate the Committee's continued support for that mission. In the words of Bear Bryant, "defense wins championships."

Enhanced Cybersecurity Services ("ECS") and Einstein 3 Accelerated ("E3A")

One of the most critical roles the Department of Homeland Security can play is to leverage the classified cyber threat indicators the federal government gathers through law enforcement, intelligence collection and other government-specific functions to protect private sector critical infrastructure and government networks. This is no small task because the cyber indicators themselves must be protected from our adversaries in an end-to-end secure environment and put to use in the field without compromising the sources and methods that yielded them in the first pace. To do this, DHS has developed two programs:

- Enhanced Cybersecurity Services ("ECS") for private sector critical infrastructure providers as well as state and local governments, and
- Einstein 3 Accelerated ("E3A") for federal civilian networks.

With both programs, Internet service providers like CenturyLink, under the direction of DHS personnel, administer intrusion prevention and threat-based protections on traffic entering and leaving the networks of participating organizations. Participation is voluntary, and non-federal participants in ECS must first be validated by DHS, but those who do participate receive an elevated level of protection from the most sophisticated cyber intruders.

CenturyLink has worked extensively with the federal government to develop these programs, and provide important protections against the most advanced threats while educating the government on practical aspects of providing such services to private industry. Expanding the scale and automating the information gleaned within "circles of trust" is the next critical step in providing effective and time critical cybersecurity protections to government and critical infrastructure providers.

State and local governments administer many functions that are important to public safety and the protection of critical infrastructure, however, they continue to lag in funding mechanisms. DHS has taken the lead to fill this gap temporarily in their support for MS-ISAC services, but additional funding for additional services such as ECS would help state governments avoid becoming the “weak link” with their federal partners.

Developing the Cybersecurity Workforce

CenturyLink appreciates the Department of Homeland Security’s leadership on developing the nation’s cybersecurity workforce, including its support for teacher training and university research and curriculum development in Louisiana. Especially in the last year, CenturyLink has focused on developing and attracting a broad range of innovation professionals, including engineers, senior IT personnel, product managers, researchers and others to help staff our Technology Center of Excellence, which will open early next year.

Our headquarters are located along the I-20 Corridor that spans northern Louisiana and is home to a number of innovation hubs, including the National Center for Academic in Information Assurance Education at Louisiana Tech University, the Cyber Information Technology program at Bossier Parish Community College, and the Cyber Innovation Center, a research park and nonprofit organization devoted to building the knowledge-based workforce in the region. Computer Sciences Corporation recently announced plans to bring 800 new jobs to the Cyber Innovation Center, and we are hopeful that as businesses step up investment in the region, we can work together to cultivate a world class cyber workforce. We would encourage this Committee and DHS to place a renewed emphasis on workforce development in the cyber arena by addressing the potential shortage of qualified and skilled employees that will be needed.

We also support the National Integrated Cyber Education Research Center (NICERC) at the Cyber Innovation Center, which focuses on curriculum design, professional development, and collaboration in K-12 and college education. NICERC has organized programs to give teachers the training and tools to prepare students for a career in cyber security, including problem-solving, critical thinking and communication skills. Of special note, NICERC is the lead technical institution for DHS’s Cybersecurity Education and Training Assistance Program (CETAP) – so the teacher-focused cybersecurity education model first developed and implemented by NICERC in Louisiana can benefit school districts across the nation.

Conclusion

While the challenge of building a cyber workforce and protecting the nation’s critical infrastructure from growing threats is a daunting and multifaceted one, we are encouraged by the commitment of the White House, DHS and this Committee to bring the right resources to bear. We appreciate the determination and attention that Chairwoman Landrieu and the committee members have brought to the issue and look forward to working with you and the authorizing committees as you support and guide DHS in its mission.