Testimony of David Mahon
Vice President and Chief Security Officer, CenturyLink, Inc.
before the
Subcommittee on Communications and the Internet
Committee on Energy and Commerce
United States House of Representatives

Wednesday, March 7, 2012

Chairman Walden, Ranking Member Eshoo and members of the Subcommittee, thank you for the opportunity to testify today on this important topic. CenturyLink provides communications services to over 14 million homes and businesses in more than 37 states and around the world, including voice, broadband, video entertainment and data services, as well as fiber backhaul, cloud computing and managed cybersecurity solutions. Our customers range from the most basic voice and internet customers, to the largest Fortune 500 companies and multiple, large government agencies.

As Vice President and Chief Security Officer for CenturyLink, I am responsible for all corporate security functions including information security, critical infrastructure protection, physical security, network fraud, industrial security, workplace violence prevention, support for the National Security Telecommunications Advisory Committee (NSTAC) and DHS National Coordinating Center (NCC) as well as liaison with federal and state law enforcement and homeland security agencies.

Before joining CenturyLink, I worked for over 30 years for the FBI and was responsible for investigative teams and programs related to targeted attacks on the Internet, computer systems and networks exploited by terrorist organizations, criminal and intelligence operations of foreign governments, white collar crime investigations, and crisis management.

The cyber threat is real and serious

We are here today because members of this subcommittee and leaders in the communications industry recognize how important the issue of cybersecurity is to securing the nation's critical infrastructure, protecting consumers, fighting crime and protecting national security. Our networks, and those of our customers, are the targets of thousands of cybersecurity events daily, from simple port scans probing network defenses to sophisticated attacks. CenturyLink and our customers invest significant resources in constant and ongoing efforts to keep those assets secure.

The major cyber threats faced by the public and private sector generally fall into four categories: Nation-state sponsored intrusions (also known as "advanced persistent threat"); Criminal, which extends to sophisticated organized crime; "Hacktivism"; and Insider attacks. Reports in the media, and private industry and government studies have documented the extensive threats to corporations, consumers and government agencies.

As a leading national network provider, CenturyLink utilizes an overarching governance, risk and compliance (GRC) framework to ensure cybersecurity threats are addressed enterprise-wide. This GRC framework allows CenturyLink to advance and evolve its information security program to identify, mitigate and remediate risks related to our corporate and customers' data, networks and systems.

The roles of communications providers

Communications providers are just one part of the cyber ecosystem, so our cybersecurity efforts are just one part of a comprehensive effort that includes technology providers, end users, owner/operators of critical infrastructure, and our government partners. As stewards of the Internet infrastructure, CenturyLink's programs on cybersecurity fall into several general categories:

Protecting the consumer experience.
As hackers, criminals and other entities seek to prey on our customers by exploiting the Internet's open architecture, CenturyLink has worked within the Internet community on measures we can take to mitigate this situation. For instance, when we learn from third-party partners that our customers' computers are likely infected with malware that makes them part of a "botnet," we notify the customers and direct them to resources to help them clean up the malware. This is a free program we launched in 2006 to improve our customer experience and minimize abuse of our network. We notify tens of thousands of customers with infected computers each year, and provide education and remediation tools. We have shared our program and experiences with other ISPs globally and are currently working with the industry on voluntary industry standards to help address the overall botnet problem.

For residential consumers, we provide educational material, anti-virus protection, malware notification and self-help mitigation tools, firewall, and parental controls as part of their ISP service. We also offer fee-based services for customers who need assistance keeping their computers running efficiently along with cleaning malware from their systems

In addition, we are actively engaged in addressing issues in Domain Name System (DNS) and Border Gateway Protocol (BGP) security. We are working with stakeholders and other industry partners on new BGP security standards that we hope will help prevent accidental and malicious Internet route hijacking. We have also worked for the past several years on DNS security by improving the monitoring of the current DNS system while working with industry leaders in developing practical implementations of DNSSEC security.

Protecting our core networks.
As a major communications provider, whose customers expect security and reliability, we are ever mindful that our networks are potential targets. Our security protocols continue to evolve with the increasing sophistication of cyber

attacks and include continuous monitoring, testing and upgrades of our practices and infrastructure to protect our networks. We have a direct and strong economic incentive to keep our networks secure and our services available.

Providing managed cybersecurity and secure communications services. CenturyLink provides a wide range of managed security services to a number of critical infrastructure clients, including government agencies, financial services, transportation and energy providers. We also provide national and international secure cloud computing services and diversified, secure communications paths to ensure reliable and available communications access to those services.

Public-private partnerships

CenturyLink has been an operational and collaborative partner with government for more than 25 years and is a Resident Member of the DHS National Coordinating Center. In the past ten years, we have worked extensively with our industry peers, partners in government and other stakeholders to strengthen our collective defenses against cyber attacks. From our CEO's participation on the President's National Security Telecommunications Advisory Committee, to my security team's participation in key organizations such as the Communications Sector Coordinating Council (CSCC), the FBI's Domestic Security Alliance Council (DSAC), and InfraGard Program, our goal is to share the information we can in order to make our network and the entire communications infrastructure more secure and connected.

We are also members of the National Cyber-Forensics Training Alliance (NCFTA), which functions as a conduit between private industry and law enforcement with a core mission to identify, mitigate and neutralize cyber crime. Once a significant online scheme is realized, an initiative is developed wherein the NCFTA manages the collection and sharing of intelligence with the affected parties, industry partners, appropriate law enforcement agencies, and other subject matter experts. In addition, we work extensively with our industry peers, operating system developers, and other private security organizations through the Network Security Information Exchange (NSIE) to ensure the security of our network and customer information.

The government has worked to step up its game as well. From President Bush's Homeland Security Presidential Directive 7 (HSPD-7) to President Obama's 2009 Cyberspace Policy Review, our national leaders have been evolving the government response to cybersecurity. Public-private partnerships and stakeholder programs organized through the Department of Homeland Security (DHS), the FCC, the FBI, Department of Defense and other agencies have focused on a number of key areas where industry and government can strengthen each other's efforts. We participate in many of these programs.

- We are currently working with DHS and other agencies to update the 2008 National Sector Risk Assessment, which will identify potential areas for

continued collaboration between government and the private sector to mitigate cyber threats to the communications industry.

- As a resident member of the DHS National Coordinating Council, CenturyLink maintains an employee presence within National Cybersecurity and Communications Integration Center (NCCIC), to coordinate in real time with government partners in the event of a cyber emergency.

- Working with DHS, CenturyLink, and other members of the Communications Sector, helped develop the National Cyber Incident Response Plan (NCIRP). As part of that effort, CenturyLink helped to develop the roles that industry partners would play in the event of a cyber emergency, and is a designated member of the Unified Coordination Group referenced within the plan.

- We have participated in a number of cyber exercises, including the DHS's biennial "Cyber Storm" exercises, and will be participating in the upcoming National Level Exercise (NLE) 2012. Through these efforts, we seek to better understand the roles each party would play, with the goal of refining the incident response plans.

- We are working through the National Institute for Standards and Technology (NIST) and a number of other industry-centric standards bodies to develop standards and best practices on cybersecurity.

- CenturyLink CEO Glen Post chairs the FCC's Communications, Security, Reliability and Interoperability Council (CSRIC), which is working on voluntary best practices for botnet remediation, domain name system security ("DNSSEC"), Internet route hijacking and other emerging issues unique to the communications industry.

More can and should be done – but carefully

Public-private partnerships have yielded significant progress in the last few years by building a framework for collective defense and cooperation, and helping us understand the cyber threat. Additional progress to improve the nation's cyber defenses will come from continued robust commitment to the partnerships and activities that are already underway.

As many have pointed out, however, we are entering into a new era of cybersecurity threats where our adversaries have become more sophisticated and determined, and the need to collectively step up our game is more acute. We are particularly encouraged by legislation like HR 3523, the Cyber Intelligence Sharing and Protection Act, and similar provisions in Senate bills that could clarify and enhance cyber-related, public-private information sharing. As communications providers, we see a number of areas where congressional action can make valuable improvements to our nation's cybersecurity posture as follows:

Improving information sharing

Information sharing with government and between industry can be improved through legislation, with appropriate privacy protections.

- Clarifying that sharing of cyber threat information among private sector entities is permitted and encouraged.
- Allowing government to reasonably share classified information with cybersecurity providers to enhance protection of critical infrastructure.
- Expediting security clearances and space accreditations to support and expand programs that would use classified information to protect information networks.

Market-based incentives and gap analyses

Market-based incentives and gap analyses can incentivize continued improvement among the private sector. For example, providing liability protection and appropriate antitrust safe harbors for cyber threat information sharing, as well as assurances that cybersecurity disclosures to the government won't be used as excuses for more regulation, would help make public-private partnerships more effective. As cyber threats evolve, regularly updating the communications providers on evolving risks and threats would play a critical role in identifying "gaps" between our current efforts and any incremental defenses needed to focus both government and private sector resources more effectively.

Improving the federal government's cybersecurity posture

We believe reforming the Federal Information Security Management Act (FISMA) through deployment of government-wide managed security solutions and a more active management role for DHS, can protect government networks more effectively.

Expanded research and development

Research and development is necessary to develop new methods of threat mitigation. With clearly defined information sharing policies and procedures with liability protections, ISPs can work more closely with both the affected businesses and government to develop innovative new solutions, and deliver them to the market place more quickly.

Shifting to a mandate-based approach would be counterproductive

We strongly caution against a traditional regulatory approach based on government mandates or "performance requirements." Because our network is the one central asset of our business, CenturyLink and our industry peers already have the strongest commercial incentives to invest in, and maintain robust cybersecurity. There is neither a lack of will nor a lack of commitment to do this among the major communications providers.

At its best, cybersecurity is a dynamic, constantly evolving challenge, best done in a collaborative partnership. At its worst, cybersecurity can devolve into a checklist exercise that diverts resources away from effective, evolving protections, into expensive compliance measures that may be already outdated by the time they are implemented. We have the most knowledge of our network, systems and databases, and we understand the most effective and efficient ways to protect these assets. Our goal-oriented approach to cybersecurity strives to ensure the availability and integrity of our networks and the transactions that go across our networks.

Conclusion

We commend the members of the Energy and Commerce Committee for their interest in improving the nation's cybersecurity, and for the deliberative process the committee is undertaking to find the right mix of incentives and elimination of legal barriers. CenturyLink has strived to be a constructive partner in this effort and will continue to do so.