Statement of the Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
Hearing on "Cybersecurity: The Pivotal Role of Communications Networks"
March 7, 2012

(As Prepared for Delivery)

Back in October, the *House Republican Cybersecurity Task Force* recommended that the committees of jurisdiction review cybersecurity issues. This subcommittee has embarked on a series of hearings to heed that call and to get a complete picture of the cybersecurity challenges our nation faces. In our February 8 hearing, we examined threats to communications networks and the concerns of the private sector security firms helping to secure communications networks. That hearing provided us with valuable information and even some potential solutions. This hearing continues our subcommittee's review of cybersecurity issues with a focus on the steps that network operators have taken to secure their networks and any recommendations they may have on how Congress can help in those efforts.

As we heard in the February 8 hearing, threats to communications networks have come a long way in a short time. Before coming to Congress, I spent 22 years as a radio broadcaster. As a small businessman, I had to worry about securing our communications network, but those were simpler times. In modern communications networks of all types, cybersecurity has become a pressing concern. In the February 8 hearing, we heard about the dizzying array of new cybersecurity threats, like supply chain vulnerabilities, botnets and Domain Name System spoofing.

On the brighter side, we were also told during that hearing about several potential solutions to make communications networks more secure. This is why I have asked a number of my colleagues to serve on the Communications and Technology Cybersecurity Working Group. The working group is a bipartisan team of six subcommittee members – led by Subcommittee Vice-Chairman Lee Terry and Subcommittee Ranking Member Anna Eshoo – that will look into some of these potential solutions and the legal and regulatory impediments to securing communications networks against cyberthreats. With an eye toward incentive-based approaches, the working group looks to facilitate communication among private sector companies and with the public sector on a variety of topics, including DNSSEC adoption, supply chain risk management, and a voluntary code of conduct and best practices for network operators.

In this hearing, we are privileged to have five witnesses that represent parts of the commercial network to guide us through the complex cybersecurity issues that they face. Network operators own, maintain, and operate most of the infrastructure that make up our communications networks. Their management of the wires, the towers, the base stations, the servers, and the wireless handsets that are integral parts of communications networks put these companies on the front lines of cybersecurity. I want to know what cybersecurity services and educational initiatives are being aimed at consumers, what steps are being taken to secure the

core components that make up our communications networks, and what affirmative steps network operators have taken to secure the supply chain and to prevent cyberattacks.

I also expect to hear what you think the appropriate role of the federal government is to combat cyberthreats. Are federal laws and regulations helping or hindering information sharing? Are there cybersecurity solutions that your company has identified that would prevent cyberattacks, but would run afoul of existing laws? How can the federal government incent network operators and other members of the private sector to invest and innovate in the cybersecurity arena?

I thank the panelists for their testimony today, and I look forward to a lively discussion of these issues.