PSHSBulletin

A Publication of the Public Safety and Homeland Security Bureau

February 2012

The FCC's Role in Cybersecurity

by Jane Kelly

The FCC is committed to taking effective, measured steps to protect the security and reliability of the Nation's communications networks. Cyber threats present growing challenges to the constantly evolving technology present in these networks. The FCC has focused its efforts in three specific areas that we feel will effectively combat these new challenges. Cybersecurity is an important topic that encompasses everything from keeping our credit card information secure to securing our Nation's critical infrastructure. It affects everyone, and each of us has a role to play in making cyber space a more secure environment. As individuals, we each must be responsible for keeping safeguards, such as virus protection on our computer updated, as well as setting strong passwords and changing them periodically. Online businesses have an obligation to keep their customers' information secure.

As the agency charged with ensuring the security and reliability of the Nation's communications infrastructure, the FCC's role is focused primarily on securing the Nation's commercial networks over which much of our daily Internet traffic travels.

In a speech at the Bipartisan Policy Council, Chairman Genachowski outlined the FCC's plan to use our longstanding partnerships with private communications and Internet service providers to address this problem and called on these private entities to support our efforts. The Chairman's speech has been met with widespread support. And while in some ways, it marks the beginning of our involvement with ever changing cybersecurity threats; it was the culmination of a great deal of work here at the Commission.

Photos (right): Chairman Genachowski outlines the FCC's Cybersecurity plan during his speech at the Bipartisan Policy Council on February 22, 2012.

Among those in the audience were General Mike Hayden, Melissa Hathaway, BPC President Jason Grumet and Rob Strayer, BPC's Director of the National Security Preparedness Group, PSHSB Bureau Chief Jamie Barnett and Deputy Bureau Chief Jennifer Manner.

cont'd on next page ▶

The FCC's Role in Cybersecurity, cont'd.

by Jane Kelly

Many months ago, we identified three areas that we felt must be secured to protect the Nation's communication's infrastructure: the Domain Name System, Border Gateway Protocol and Botnets causing distributed denial-of-service attack. We charged our federal advisory committee, the Communications Security, Reliability and Interoperability Council (CSRIC) with tackling these difficult issues and recommending voluntary solutions. The CSRIC is an impressive group, composed of leaders from industry, academia and other government agencies who all work on the cutting edge of cybersecurity.

The Domain Name Systems – or "DNS" -- is the telephone book of the internet; the system that translates Web site names (for example, www.fcc.gov) to numerical IP addresses (for example, 201.96.10.10) that are used to find Internet sites. Domain name fraud occurs when a destination address is faked so that traffic is sent to a fraudulent or impostor website under the control of the attacker. "DNSSEC" are Domain Name System Security Extensions that address vulnerabilities in the DNS, prevent domain name fraud, and thereby, improve DNS security. DNSSEC is being used by several large Internet service provider (ISP) and government agencies. Deploying DNSSEC will help mitigate attacks, including those that enable attackers to redirect unsuspecting Internet users to malicious websites. The CSRIC is developing best practices that will guide ISPs' DNSSEC implementation. The CSRIC will also recommend performance metrics to measure the success of their efforts in promoting DNSSEC implementation among ISPs.

Border Gateway Protocol (BGP) enables users to connect with websites and Web addresses. If this protocol is not secure, Internet traffic directed at one site can be routed through another path, allowing information to pass through the hands of people who can "eavesdrop" and steal information. Obviously, Internet route hijacking can endanger valuable intellectual property, other personal property, and, more important, jeopardize our national security. We have asked the CSRIC to develop a core set of voluntary best practices that would expedite the implementation of secure routing protocols and develop best practices to minimize the likelihood and impact of BGP exploits. These best practices will be the products of the lessons learned from past problems and deliberate attacks. The working group has also been asked to develop performance metrics to measure the effectiveness of their work.

A botnet is a network of computers that become infected with malicious software – or "malware." Infected computers, called "zombies," can be controlled by bad guys launching cyber attacks without the owner of the computer ever knowing. In a botnet attack, millions of simultaneous requests to a target website, which is intended to overwhelm the site, cause it to crash, and prevent access to the site, effectively shutting down the online target businesses or entity. Thus far, botnets have cost the world wide economy billions of dollars and have even affected Federal government websites such as the FBI and the Department of Justice. To address the botnet threat, the CSRIC is proposing a voluntary Code of Conduct for ISPs. The Code of Conduct will identify best practices that can be instituted industry wide to provide a critical baseline of security to all Internet users; this has not existed to date.

The commitments we have received from the private sector to work with us in combating these threats is a huge step forward, but is still only the beginning. We must remain vigilant to these ever changing threats as we seek to secure the communications networks that grow ever more dependent on broadband technology.

Upcoming Events

- March 21, 2012 - Open Commission Meeting, FCC Headquarters, Washington, DC

For more information about the Public Safety and Homeland Security Bureau,
visit our webpage at http://www.fcc.gov/public-safety-homeland-security-bureau or email us at pshsbinfo@fcc.gov.

Questions or Comments? Email your questions or comments concerning the content of this bulletin to Kim Anderson (kim.anderson@fcc.gov).