FCC CHAIRMAN CALLS ON INTERNET COMMUNITY TO ADDRESS SIGNIFICANT CYBER THREATS TO OUR ECONOMIC FUTURE AND NATIONAL SECURITY: BOTNET ATTACKS, DOMAIN NAME FRAUD, AND INTERNET ROUTE HIJACKING

FCC Chairman Julius Genachowski joined General Michael V. Hayden (Ret.) at the Bipartisan Policy Center to outline ways the multiple stakeholders that govern the Internet can address three significant cybersecurity threats to commercial communications networks – botnets, domain name fraud and Internet route hijacking. Recognizing the Internet is an open platform for innovation and opportunity, Genachowski urged the multi-stakeholder Internet community to find industry-led, non-regulatory solutions to secure our nation's networks. These solutions include developing and adopting an industry-wide Code of Conduct to combat botnet attacks, developing secure routing standards, and beginning to implement DNSSEC. Taking steps to address major vulnerabilities in commercial networks will contribute to economic growth, encourage the wider adoption of broadband, protect the enormous opportunities created by the Internet, and bolster the broader cybersecurity endeavors of the FCC's federal partners.

Cyber criminals can wreak significant financial harm on businesses and consumers:

- Almost three-fourths of small and medium businesses report being affected by cyber attacks. (Symantec).
- A report by Gartner found 3.6 million Americans get redirected to bogus websites in a single year, costing them $3.2 million. (Gartner).
- An estimated 8.4 million credit card numbers are obtained fraudulently online every year. (Ponemon Institute).

The Internet is growing increasingly vulnerable to three major types of attack – botnets, domain name fraud and Internet route hijacking:

- **Botnets**: Robotic networks ("botnets") attack by infecting computers with malicious software ("malware"), allowing the computer to be controlled remotely. Criminals commonly use these botnets to launch cyber attacks. They can direct the infected computers to send millions of simultaneous requests to a target website, crashing the site. Legitimate site users are denied access to the website, leading to potential losses. Botnets can also be used to steal passwords and financial information.
- **Internet Route Hijacking:** The Internet is a network of networks. Connectivity between these networks is based on an implicit trust that is the Internet's greatest strength, but can also be a major weakness. The protocol that enables seamless connectivity – known as Border Gateway Protocol (BGP) – doesn't have built-in mechanisms to protect against cyber attacks. This makes it possible for bad actors to misdirect Internet traffic to untrustworthy networks.
- **Domain Name Fraud:** The Domain Name System (DNS), essentially a digital phone book for the web, has vulnerabilities that can allow the identifying information to be changed. When bad actors change the indentifying information, computer users attempting to go to one website can get misdirected to a fraudulent website.

Through its Federal Advisory Committee, the Communications, Security, Reliability and Interoperability Council (CSRIC), chaired by Glen Post, CEO and President of CenturyLink, the FCC has identified these cybersecurity threats and CSRIC is working to develop voluntary, industry-wide best practices to address network vulnerabilities, including:

- An industry-wide, voluntary anti-botnet Code of Conduct for ISPs to combat threat and protect the public.
- ISPs are urged to support the development of secure routing standards to combat internet route hijacking and plan to implement them when they are ready.
- DNSSEC is an add on to the DNS protocol, and all broad providers are urged to begin implementing DNSSEC as soon as possible.

The FCC, as the nation's expert agency on the security and reliability of communications networks, is focused on smart, practical, industry-based and voluntary best practices to minimize cybersecurity threats. The FCC recently:

- Tasked CSRIC with making recommendations in the spring of 2012 to help address critical private sector Internet security vulnerabilities.
- Working with the Small Business Administration and others, developed and released a Cybersecurity Tip sheet for small businesses, describing a number of commonsense steps small businesses can take to increase their security. http://www.fcc.gov/cyberforsmallbiz.
- With its partners, released the Small Biz Cyber Planner, an easy-to-use online tool to help small businesses to create their own customized cybersecurity plan -- http://www.fcc.gov/cyberplanner.
- Convened a roundtable event with leaders from across the public, private, and nonprofit sectors to deliver cybersecurity strategies to small business owners -- http://www.fcc.gov/events/cybersecurity-roundtable-protecting-small-businesses.