NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC. 515 F 2d 385 (D.C. Circ 1974).

FOR IMMEDIATE RELEASE:
March 22, 2012

NEWS MEDIA CONTACT:
Neil Grace, 202-418-0506
neil.grace@fcc.gov

FCC ADVISORY COMMITTEE ADOPTS RECOMMENDATIONS TO MINIMIZE THREE MAJOR CYBER THREATS, INCLUDING AN ANTI-BOT CODE OF CONDUCT, IP ROUTE HIJACKING INDUSTRY FRAMEWORK AND SECURE DNS BEST PRACTICES

Chairman Genachowski applauds voluntary commitments by nation's largest Internet Service Providers, including AT&T, CenturyLink, Comcast, Cox, Sprint, Time Warner Cable, T-Mobile and Verizon to better secure their communications networks and protect consumers and business

Washington, D.C.—Today, an industry advisory group for the Federal Communications Commission (FCC), the Communications, Security, Reliability, and Interoperability Council (CSRIC), unanimously adopted recommendations for voluntary action by Internet service providers (ISPs) to combat three major cyber security threats, including botnets, attacks on the Domain Name System (DNS), and Internet route hijacking. FCC Chairman Julius Genachowski applauded the public commitments of many of the nation's largest ISPs to implement these best practices.

CSRIC is a federal advisory committee established at the direction of the FCC Chairman to provide recommendations regarding the security, reliability, and interoperability of the nation's communications system. Currently, CSRIC is composed of more than 50 communications experts from the private sector (including ISPs), public safety, consumer organizations and tribal, local, state and federal governments.

Chairman Genachowski said, "The recommendations approved today identify smart, practical, voluntary solutions that will materially improve the cyber security of commercial networks and bolster the broader endeavors of our federal partners."

CSRIC Chair and CEO and President of CenturyLink, Glen F. Post, III, said, "I commend the industry for recognizing the importance of these voluntary initiatives and the continued willingness to work cooperatively to seek meaningful solutions."

Miriam Perlberg, Senior Director for Cybersecurity Policies on the National Security Staff, congratulated the CSRIC on its voluntary, multi-stakeholder and industry-based approach. She stated, "Successfully combating botnets is a whole of government and whole of industry approach. The White House believes, as the CSRIC's recommendations make clear and Commerce's data supports, a multi-stakeholder approach is needed to notify, educate, remediate and measure botnet threats to consumers."

Implementing a recommendation of the National Broadband Plan, CSRIC was tasked with developing measures for ISPs to mitigate three major cyber threats: botnet attacks, domain name fraud, and Internet route hijacking. Today, the advisory committee endorsed industry-based recommendations in each of these three areas, including:

- **Anti-Bot Code of Conduct:** To reduce the threat of botnets in residential networks, CSRIC recommended a voluntary U.S. Anti-Bot Code of Conduct for Internet Service Providers (Anti-Bot Code). Under the Anti-Bot Code, ISPs agree to educate consumers about the botnet threat, take steps to detect botnet activity on their networks, make consumers aware of botnet infections on their computers, offer assistance to consumers whose computers are infected and collaborate with other service providers that have also adopted the Anti-Bot Code.

- **DNS Best Practices:** CSRIC recommended that ISPs implement best practices to better secure the Domain Name System. DNS works like a telephone book for the Internet, but lack of security for DNS has enabled spoofing, allowing Internet criminals to coax credit card numbers and personal data from users who do not realize they are on an illegitimate website. DNSSEC is a set of secure protocol extensions that prevent such fraudulent activity. This recommendation is a significant first step toward full DNSSEC implementation by ISPs and will allow users, with software applications like browsers, to validate that the destination they are trying to reach is authentic and not a spoofed website.

- **IP Route Hijacking Industry Framework:** CSRIC recommended an industry framework to prevent Internet route hijacking, which is the erroneous routing of Internet traffic through potentially untrustworthy networks. CSRIC recommended that ISPs work to implement new technologies and practices to reduce the number of these events, thereby ensuring that users in the U.S. can be more confident that their Internet traffic will not be exposed to scrutiny by other networks, foreign or domestic, through misrouting.

Chairman Genachowski strongly reiterated that privacy must not be compromised for the sake of security. He also announced that CSRIC is being tasked with preparing future recommendations to ensure that the best practices endorsed today will protect the privacy of Internet users. Last month, Chairman Genachowski urged the multi-stakeholder Internet community to find industry-led, non-regulatory solutions to secure our nation's networks.

In response, several of the nation's largest ISPs participating in CSRIC, including AT&T, CenturyLink, Comcast, Cox, Sprint, Time Warner Cable, and Verizon, pledged today to implement the CSRIC recommendations. Other ISPs, such as T-Mobile, have agreed to implement those recommendations that apply to their network architecture. When fully implemented, these measures will strengthen the security of the networks of the ISPs that provide Internet access to over 50 percent of residential broadband users.

As the nation's expert agency on communications, the FCC has long history of engagement with private and public sector partners on network reliability and security. Voluntary, multi-stakeholder actions exemplified by CSRIC's recommendations, and the corporate commitments announced today, are the most effective approach for securing our networks while preserving the Internet as an open platform for innovation and communication.

-FCC-

News and information about the Federal Communications Commission is available at www.fcc.gov.