FEDERAL ADVISORY COMMITTEE UNANIMOUSLY APPROVES RECOMMENDATIONS TO COMBAT THREE MAJOR CYBERSECURITY THREATS: BOTNET ATTACKS, DOMAIN NAME FRAUD AND IP ROUTE HIJACKING

FCC CHAIRMAN JULIUS GENACHOWSKI APPLAUDS VOLUNTARY INDUSTRY COMMITMENTS BY NATION'S LARGEST ISPs

AT&T, CENTURYLINK, COMCAST, COX, SPRINT, TIME WARNER CABLE, T-MOBILE, AND VERIZON COMMIT TO IMPLEMENTING RECOMMENDATIONS

Communications, Security, Reliability, and Interoperability Council (CSRIC) Chair and President and CEO of CenturyLink Glen F. Post III presented FCC Chairman Julius Genachowski industry-based recommendations addressing three major cybersecurity threats to commercial networks. Chairman Genachowski applauded the commitments by the nation's largest Internet Service Providers (ISPs) to implement the recommendations, including an Anti-Bot Code of Conduct, secure DNS best practices and an IP route hijacking industry framework. CSRIC's vote delivered on the Chairman challenge to the multi-stakeholder Internet community to produce industry-led, non-regulatory solutions to cyber threats to strengthen the security of the communications networks used by tens of millions of Americans every day.

CSRIC, the Federal Advisory Committee, unanimously endorsed voluntary, industry-wide best practices to address three major network vulnerabilities that allow cyber criminals to access Internet traffic for nefarious purposes such as the theft of personal information and intellectual property, including:

1. **Botnets:** The growth of bot-infected end-computers poses a threat to the vitality and resiliency of the Internet and to the online economy. Botnets are networks of computers infected with bot malware, which can be controlled remotely. Criminals often use botnets to crash or deny access to a target website, and botnets can be used to steal passwords and financial information.

   ***Solution**: **Anti-Bot Code of Conduct**: The CSRIC recommended ISPs participate in a U.S. Anti-Bot Code of Conduct that encourages ISPs to engage in: (1) end-user education to prevent bot infections; (2) detection of bots; (3) notification of potential bot infections; (4) remediation of bots; and (5) collaboration and sharing of information. The Code, when implemented by ISPs, should reduce the number of infected computers and help to protect users from identity theft and fraud.*

2. **Domain Name Fraud:** DNS works like a telephone book for the Internet, converting easily remembered domain names (for example, www.fcc.gov) to numerical IP addresses (for example, 201.96.10.10). 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 have been sent to an illegitimate website. DNSSEC is a set of secure protocol extensions that prevent such fraudulent activity.

   ***Solution: Domain Name System Best Practices:** The CSRIC recommended that ISPs take the first step to full DNSSEC implementation that will allow web users, with software applications like browsers, to validate that the destination they are trying to reach is authentic and not a spoofed website.*

3. **Internet Route Hijacking:** The protocol that allows seamless connectivity between the network of networks that make up the internet, Border Gateway Protocol (BGP), does not have built-in security measures. Internet traffic can be misdirected through potentially untrustworthy networks such as those operated by cyber criminals or by foreign governments.

   ***Solution: IP Route Hijacking Industry Framework:** CSRIC recommended the development of an industry framework to prevent Internet route hijacking, which will implement new technologies and practices to*

reduce the number of these events, thereby enabling users to be more confident that their Internet traffic will not be exposed to scrutiny by other networks through misrouting

Looking forward, CSRIC will build on these best practices to ensure their successful implementation.

- CSRIC has been tasked with developing ways to measure the effectiveness of the three sets of recommendations adopted today.
- CSRIC is being newly tasked with producing recommendations to ensure that these best practices are implemented in a manner that protects the privacy of Internet users.

There is widespread industry support for the FCC's voluntary multi-stakeholder approach and the resulting recommendations by the CSRIC.

- Many of the nation's largest ISPs providing service to the majority of residential broadband users agreed to implement the best practices approved by CSRIC.
- The companies committing to implement as appropriate CSRIC's recommendations include AT&T, CenturyLink, Comcast, Cox, Sprint, Time Warner Cable, T-Mobile and Verizon.

The FCC is the nation's expert agency on communications technology and the security and reliability of communications networks has always been a part of the agency's fundamental mission. The agency is uniquely situated to work with both the public and private sectors on addressing network vulnerabilities.

- The FCC has a long history of working with the companies that operate the core of the Internet on network reliability and security issues.
- Working with its federal partners the FCC has developed tools for small business owners to increase their cybersecurity. http://www.fcc.gov/cyberforsmallbiz
- Working with the Small Business Administration and others, the FCC released a cybersecurity tip sheet for small businesses. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf
- With its partners, the FCC created an easy online tool to help small businesses create their own customized cyber security plan. http://www.fcc.gov/cyberplanner.
- Convened roundtable event with leaders from across the public, private, and nonprofit sectors to deliver cyber security strategies to small business owners. http://www.fcc.gov/events/cybersecurity-roundtable-protecting-small-businesses.