PUBLIC NOTICE

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

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

DA 14-1066
Released: July 25, 2014

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON IMPLEMENTATION OF CSRIC III CYBERSECURITY BEST PRACTICES

In March 2012, the FCC's third Communications Security, Reliability and Interoperability Council (CSRIC III)[1] unanimously adopted voluntary recommendations for Internet service providers (ISPs) to combat three major cybersecurity threats: (1) botnet attacks; (2) domain name fraud; and (3) Internet route hijacking.[2] Among other stakeholders, leading ISPs participated in the development of these recommendations and publicly committed to implementing them.[3] The recommendations included voluntary measures in three areas: an Anti-Bot Code of Conduct to mitigate the proliferation of distributed denial of service (DDoS) attacks,[4] steps to better secure the Domain Name System (DNS) through incremental implementation of DNSSEC, and steps to strengthen the security of the Internet's inter-domain routing infrastructure.[5]

CSRIC III also recommended that the FCC encourage ISPs to implement source-address filtering to prevent attackers from spoofing IP addresses to launch DDoS attacks. Specifically, CSRIC recommended that the FCC encourage implementation of the following best current practices (BCPs) to mitigate this risk:[6]

1) BCP 38/RFC 2827 – Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing;[7] and

2) BCP 84/RFC 3704 – Ingress Filtering for Multi-homed Networks.[8]

All CSRIC best practices are available on the Commission's website in a searchable database.[9]

Since CSRIC III adopted these important recommendations, stakeholders have not yet provided the FCC's Public Safety and Homeland Security Bureau (Bureau) information regarding their implementation that is sufficient for a meaningful understanding of either their effectiveness or lessons learned from implementation. Meanwhile, the vulnerabilities these recommendations were intended to address continue to be exploited.[10] For example, recent DDoS attacks of unprecedented scale[11] add to the urgency of ISPs' implementation of CSRIC recommendations or of alternative approaches that ISPs believe are superior to the CSRIC recommendations.

Request for Comment

By this Public Notice, the Bureau seeks comment from ISPs, the Internet community, consumer organizations, and the broader public on the implementation and effectiveness of the CSRIC III recommendations and/or alternatives that stakeholders have developed since the time of the CSRIC's original work to address these challenges.

The purpose of this Public Notice is to promote a robust, stakeholder-driven discourse drawing on broad perspectives from throughout the cyber ecosystem to provide the communications sector and the Commission new information, insights and situational awareness regarding innovative solutions to these

particular cyber risks. To the extent that companies or stakeholders may prefer that their submissions remain confidential, we intend to protect the confidentiality of submissions according to the requests and consistent with FCC rules, as described below. This inquiry is part of the Commission's effort to develop effective and proactive private sector-driven cyber risk management;[12] in particular, it complements and supports ongoing work in CSRIC IV to create measurable, accountable cyber assurances across a wide variety of IP-based communications technologies and services.[13]

The Bureau seeks public comment on the implementation status and effectiveness of these voluntary recommendations, or alternatives, by ISPs and other members of the Internet community. We are particularly interested in comment on the following questions as they relate to the four broad areas of CSRIC's previous best practices and recommendations cited above:

1. What progress have stakeholders made in implementing the recommendations?
2. What barriers have stakeholders encountered in implementing the recommendations?
3. What significant success stories or breakthroughs have been achieved in implementing the recommendations?
4. What are stakeholders' views and/or plans for full implementation of the recommendations?
5. How effective are the recommendations at mitigating cyber risk when they have been implemented? Given the experiences gained in the past two years, are there alternatives to full implementation that could be more effective than full implementation at mitigating cyber risk risks posed by botnets, DNS vulnerabilities, routing infrastructure vulnerabilities, and source address spoofing? On what basis do stakeholders believe that these alternatives are more effective than the CSRIC III recommendations? Do stakeholders undertake qualitative or quantitative evaluations of the effectiveness of these various approaches, or both?

Comment Submission

Interested parties are invited to comment by September 26, 2014. Please submit comments or meeting requests by email directly to the Associate Bureau Chief for Cybersecurity and Communications Reliability, Jeffery Goldthorp, at jeffery.goldthorp@fcc.gov, with a copy to the Deputy Chief of the Bureau's Cybersecurity and Communications Reliability Division, Lauren Kravetz, at lauren.kravetz@fcc.gov.

Requests for confidential treatment of information submitted should follow the procedures set forth in section 0.459 of the Commission's rules, under which all submissions with an appropriate request for confidential treatment will be treated as presumptively confidential pending a ruling on the request. Additionally, upon request and on a case-by-case basis, the Bureau may accommodate classified comment submissions or discussions.

Alternatively, those who desire to submit comments in hard copy only should submit an original and one copy of each set of comments. Hard copy comments can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All such submissions should be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission and reference DA 14-1066.

- All hand-delivered or messenger-delivered paper submissions for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. Delivery hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

For further information, contact Jeffery Goldthorp, at jeffery.goldthorp@fcc.gov or (202) 418-1096 or Lauren Kravetz, at lauren.kravetz@fcc.gov or (202) 418-7944.

– FCC –

---

[1] CSRIC is a federal advisory committee composed of leaders from the private sector, academia, engineering, consumer/community/non-profit organizations, and government partners from tribal, state, local and federal agencies. *See* FCC Encyclopedia, Communications Security, Reliability and Interoperability Council III, http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

[2] *See* CSRIC III FINAL REPORTS, WORKING GROUPS 5, 6, 7, *available at* http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

[3] *See* AT&T Public Policy Blog: Cybersecurity and the FCC's CSRIC Recommendations (March 22, 2012), *available at* http://www.attpublicpolicy.com/cybersecurity/cybersecurity-and-the-fccs-csric-recommendations/; CenturyLink Public Policy Blog: CenturyLink Takes Cybersecurity Seriously (April 2, 2012), *available at* http://community.centurylink.com/regulatoryblog/2012/04/centurylink-takes-cybersecurity-seriously/; and Comcast Voices: Comcast Applauds Work of the FCC's CSRIC on Online Security and Safety (March 22, 2012), *available at* http://corporate.comcast.com/comcast-voices/comcast-applauds-work-of-the-fccs-csric-on-online-security-and-safety.

[4] In a distributed denial-of-service (DDoS) attack, an attacker uses multiple computers to prevent legitimate users from accessing information or services by sending large amounts of data to a website or spam to particular e-mail addresses. *See* Security Tip (ST04-015), Understanding Denial-of-Service Attacks, US-CERT, (Feb. 06, 2013), http://www.us-cert.gov/ncas/tips/ST04-015. Source-address spoofing may lead to "attacks where the unreachability of the source can be exploited" by attackers who transmit packets that appear to come from a victim's IP address. *See* CSRIC III WORKING GROUP 4 FINAL REPORT at 18 (March 2013), *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf (CSRIC III WG4 REPORT).

[5] *See* News Release: 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, (March 22, 2012), *available at* http://www.fcc.gov/document/csric-adopts-recs-minimize-three-major-cyber-threats.

[6] CSRIC III WG4 REPORT at 20.

[7] *See* P. FERGUSON & D. SENIE, BEST CURRENT PRACTICE 38, NETWORK INGRESS FILTERING: DEFEATING DENIAL OF SERVICE ATTACKS WHICH EMPLOY IP SOURCE ADDRESS SPOOFING (2000), *available at* http://tools.ietf.org/html/bcp38.

[8] *See* F. BAKER AND P. SAVOLA, BEST CURRENT PRACTICE 84, INGRESS FILTERING FOR MULTIHOMED NETWORKS, (2004), *available at* http://tools.ietf.org/html/bcp84.

[9] *See* CSRIC Best Practices, FCC Public Safety and Homeland Security Bureau, https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm.

[10] *See* Jim Cowie, *The New Threat: Targeted Internet Traffic Misdirection*, RENESYS BLOG, Nov. 19, 2013, *available at* http://www.renesys.com/2013/11/mitm-internet-hijacking/. According to an Internet security firm that investigated the attack, victims included financial institutions, governments, and network service providers in the United States, South Korea, Germany, and several other countries. *Id.* *See also* Nicole Perlroth, *In Cyberattacks on Banks, Evidence of a New Weapon*, THE NEW YORK TIMES, Oct. 5, 2012, *available at* http://bits.blogs.nytimes.com/2012/10/05/in-cyberattacks-on-banks-evidence-of-a-new-weapon/. *See also* Mathew

J. Schwartz, *Bank DDoS Attacks Resume: Wells Fargo Confirms Disruptions*, INFORMATION WEEK, March 27, 2013, *available at* http://www.informationweek.com/attacks/bank-ddos-attacks-resume-wells-fargo-confirms-disruptions/d/d-id/1109271?.

[11] In a Reflective DNS Amplification DDoS attack, an attacker sends multiple requests to multiple open DNS resolvers pretending that they are coming from a victim's IP address. The open DNS resolvers then reply to the victim's IP address with larger packets thus amplifying the attack size. *See* David Piscitello, *Anatomy of a DNS DDoS Amplification Attack*, WATCHGUARD TECHNOLOGIES, INC., http://www.watchguard.com/infocenter/editorial/41649.asp. *See also* John Leyden, *Biggest DDoS Attack in History Hammers Spamhaus*, THE REGISTER (March 27, 2013), http://www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood/; John Markoff and Nicole Perlroth, *Firm Is Accused of Sending Spam, and Fight Jams Internet,* N.Y. TIMES, (March 26, 2013), *See also* Mathew J. Schwartz, *DDoS Attack Hits 400 Gbit/s, Breaks Record*, INFORMATION WEEK (Feb. 11, 2014), *available at* http://www.informationweek.com/security/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787.

[12] *See* remarks of FCC Chairman Tom Wheeler to the American Enterprise Institute, June 12, 2014 *available at* http://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc. Chairman Wheeler stated that "the pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking" and challenged communications providers to create a "new paradigm" of proactive, measurable, accountable, business-driven cyber risk management. He cited the "important foundational work" in cybersecurity from CSRIC III that is the subject of this Public Notice and announced that "in the coming weeks, we will be seeking information to measure the implementation and impact of these industry-defined best practices."

[13] *See* Remarks of Public Safety and Homeland Security Bureau Chief, Rear Admiral (Ret.) David Simpson to CSRIC IV Public Meeting, June 18, 2014, *available at* http://www.fcc.gov/events/communications-security-reliability-and-interoperability-council-iv-meeting-1. Admiral Simpson's remarks reiterated Chairman Wheeler's call for a "'new paradigm' of proactive, measurable, accountable, business-driven risk management for communications security and reliability" and further described the "new paradigm" as "a substitute for traditional regulation that is more dynamic than complying with rules and more effective than blindly trusting the market. Under this new approach, businesses would step up and take responsibility for determining how to manage their risk in a more transparent and measurable way that promotes market accountability for cyber risk reduction. The traditional regulatory approach was that the FCC would propose a rule, and, after taking in your comments, tell you what you have to do – and, then, we would measure whether or not you are doing what we told you to do. The 'new paradigm' approach is different, and it is more challenging, because if it is going to succeed, it will rely primarily on your action. This is the case both in developing best practices and risk management processes in the first place, and then in following through with meaningful, measurable, demonstrable implementation."