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 15-354
Released: March 19, 2015

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON CSRIC IV CYBERSECURITY RISK MANAGEMENT AND ASSURANCE RECOMMENDATIONS

PS Docket No. 15-68

Comment date: **May 29, 2015**
Reply date: **June 26, 2015**

By this Public Notice, the Federal Communications Commission's (FCC) Public Safety and Homeland Security Bureau (Bureau) seeks comment on the report on Cybersecurity Risk Management and Best Practices submitted by the fourth Communications Security, Reliability and Interoperability Council (CSRIC IV).[1]

As the central element of the effort to develop effective and proactive private sector-driven cyber risk management,[2] the FCC charged CSRIC IV with recommending voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across their respective enterprises.[3] Specifically, the FCC tasked CSRIC with developing recommendations on how to provide demonstrable assurances that communications providers are reducing cybersecurity risks through the application of the voluntary National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity,[4] or an equivalent construct; and to develop recommendations that are: (1) tailored by individual companies to suit their unique needs, characteristics, and risks; (2) based on

---

[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 IV, http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv (last visited Mar. 18, 2015).

[2] *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.

[3] *See* CSRIC IV Working Group Descriptions and Leadership, at 5 (charge to Working Group 4) http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20IV%20Working%20Group%20Descriptions%2010%2023%2014.pdf.

[4] The National Institute of Technology and Standards (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

meaningful indicators of successful cyber risk management; and (3) allow for meaningful assessments both internally and externally.[5]

On March 18, 2015, following an effort by over 100 cybersecurity experts from the communications sector, federal government, state government, equipment manufacturers, cybersecurity solution providers, and the financial, banking, and energy sectors, CSRIC IV unanimously adopted a detailed report that includes segment-specific analysis of the application of the Cybersecurity Framework as well as recommendations in response to the Commission's charge. The CSRIC IV "Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report" is available at http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf

The Bureau generally seeks comment on the cybersecurity risk management recommendations of CSRIC IV, and/or suggestions of alternatives to better achieve the FCC's goals. Among other things, the Bureau seeks comment on the following:

1. In what ways are the CSRIC IV recommendations sufficient to meet the FCC's goal of reducing cybersecurity risk to critical infrastructure, enterprises, and consumers? In what ways, if any, might these recommendations be improved, augmented, or made more specific?

2. These recommendations include the following voluntary mechanisms to provide assurances to provide evidence of the communications sector's commitment to enhance cybersecurity risk management capabilities. We seek comment on each as indicated:

    a. *FCC-convened confidential company-specific meetings or other communications formats.* How should the Commission prepare for and conduct these meetings to ensure that they result in information that is useful for assessing the state of cybersecurity risk management among communications providers?
    b. *A new component of the Communications Sector Annual Report that focuses on segment-specific cybersecurity risk management.* What measures should this Annual Report include to provide appropriate levels of visibility about the state of cybersecurity risk management over time?
    c. *Active and dedicated participation in DHS' Critical Infrastructure Cyber Community C3 Voluntary Program.* How should the Commission coordinate with DHS in the context of the C3 Voluntary Program to help small and mid-sized communications providers make use of the CSRIC recommendations?

3. What barriers, if any, would inhibit industry's effective application of the voluntary mechanisms discussed throughout the report? What differences exist based on factors such as size? How might these barriers be mitigated?

Interested parties may submit comments by **May 29, 2015** and reply comment**s** by **June 26, 2015** via the Commission's Electronic Comment Filing System, hard copy, and/or meetings scheduled with FCC staff as detailed below.

Procedural Matters

Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 C.F.R. §§ 1.415, 1.419, interested parties may file comments on or before the dates indicated on the first page of this document.

---

[5] *See supra note 3.*

Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See* Electronic Filing of Documents in Rulemaking Proceedings, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet, by accessing the ECFS: http://apps.fcc.gov/ecfs.

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

  Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, D.C. 20554. The filing 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.

People with Disabilities: 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 and Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (tty).

Pursuant to Part 1, Subpart H, presentations to Commission staff pursuant to this Public Notice are exempt from *ex parte* filing obligations.

Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in section 0.459 of the Commission's rules. Casual claims of confidentiality are not accepted. Confidential submissions may not be filed via ECFS, but rather should be filed with the Secretary's Office following the procedures set forth in 47 C.F.R. § 0.459. Redacted versions of confidential submissions may be filed via ECFS. Parties are advised that the Commission looks with disfavor on claims of confidentiality for entire documents. When a claim of confidentiality is made, a public, redacted version of the document should also be filed.

FOR FURTHER INFORMATION or to schedule a meeting with FCC staff, contact the Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, Steven McKinnon at (202) 418-0390 or steven.mckinnon@fcc.gov or Linda Pintro at (202) 418-7490 or linda.pintro@fcc.gov.

NEWS MEDIA CONTACT: Rochelle Cohen, at rochelle.cohen@fcc.gov, or (202) 418-1162.

The Public Safety and Homeland Security Bureau issues this Public Notice under delegated authority pursuant to Sections 0.191 and 0.392 of the Commission's rules, 47 C.F.R. §§ 0.191, 0.392.