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 18-333
Released: April 3, 2018

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REQUESTS COMMENT ON IMPLEMENTATION OF SIGNALING SYSTEM 7 SECURITY BEST PRACTICES

Comment Date: May 3, 2018
Reply Date: June 4, 2018

Introduction

In March 2017, the Federal Communications Commission's (Commission) Communications Security, Reliability and Interoperability Council (CSRIC) recommended that communications service providers implement certain security measures to help prevent exploitation of carrier Signaling System 7 (SS7) network infrastructure.[1] These recommendations were intended to increase awareness of SS7 signaling vulnerabilities, and included risk mitigation strategies for the continued use of SS7. The recommendations also listed measures, such as filtering and authentication of traffic between service provider networks, designed to promote the security of SS7 communications network traffic. Finally, CSRIC examined security practices and made recommendations related to next generation protocols that will interact with SS7 and Session Initiation Protocol (SIP) infrastructures, such as Diameter, which is the protocol that supports the accounting and authorization responsibilities of SS7 in the all-IP network and most 3G and beyond wireless networks.[2]

In August 2017, the Public Safety and Homeland Security Bureau (Bureau) released a Public Notice recommending that communications service providers implement the CSRIC best practices.[3] In order to help assess the effectiveness of these recommendations, the Bureau now seeks public comment and information on the implementation of these recommendations, including any progress, barriers, and lessons learned.

Request for Comment

[1] CSRIC is an advisory committee of the Federal Communications Commission, the mission of which is to make recommendations to the Commission to promote the security, reliability and resiliency of the Nation's communications systems. FCC, Communications Security, Reliability, and Interoperability Council (CSRIC), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited December 14, 2017). Signaling System 7 (SS7) is a signaling protocol that supports call setup, routing, exchange, and billing functions in communications networks by transmitting messages between fixed and mobile service providers.

[2] *See* CSRIC V: Working Group 10, Legacy Risk Reductions (2017) (Legacy Risk Reductions Report), https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf.

[3] *See* FCC's Public Safety and Homeland Security Bureau Encourages Implementation of CSRIC Signaling System 7 Security Best Practices, Public Notice, DA 17-799 (PSHSB Aug. 24, 2017).

The Bureau seeks public comment, including from communications service providers and other stakeholders, on the implementation and effectiveness of the March 2017 CSRIC recommendations regarding SS7 security risks. The Bureau also seeks comment on any alternatives to the CSRIC recommendations that communications service providers have implemented or plan to implement to help address SS7 security risks.

The Bureau is particularly interested in comment on the following sets of questions as they relate to the CSRIC recommendations:

1. **Progress:** CSRIC's Legacy Risk Reductions Report contained nine specific recommendations for reducing SS7 security risks and increasing situational awareness. What progress has been made by communications service providers in implementing the recommendations? To the extent communications service providers plan to implement the recommendations but have not yet done so, what are their plans to implement the recommendations? What factors have communications service providers considered in devising these implementation plans? What barriers have communications service providers encountered in implementing the recommendations? What factors have communications service providers used to determine whether any of the recommendations are not suitable for their networks?

2. **Evaluation:** What successes have communications service providers achieved by implementing the recommendations? What indicators (qualitative and quantitative) have communications service providers used to determine the correlation between implementation of the recommendations and reduction in SS7 security risks? How effective are the recommended measures in reducing SS7 security risks? Are there alternatives that could be more effective than the measures recommended by CSRIC, and if so, what are these alternatives and why are they more effective?

3. **Other Considerations:** Have communications service providers shared potential SS7 security risks with their various internal business units and key business clients that rely on SS7 signaling (*e.g.*, SMS) as well as to interconnected peer providers, and if so, how? What measures have been implemented to help protect the privacy of subscriber data from SS7 exploits? How long do communications service providers keep SS7 network logs in the normal course of business, and would longer retention times be helpful in responding to potential SS7 security compromises?

Procedural Matters

Pursuant to Sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the FCC's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 CFR 24121 (1998).

- Commenting parties may file comments in response to this Notice in PS Docket No. 18-99.
- 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.
- 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 FCC's Secretary, Office of the Secretary, Federal Communications Commission.

- All hand-delivered or messenger-delivered paper filings for the FCC's Secretary must be delivered to FCC Headquarters at 445 12th Street, SW, Room TW-A325, Washington, DC 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 9050 Junction Drive, Annapolis Junction, MD 20701.
- 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).

Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in Section 0.459 of the FCC'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 CFR § 0.459. Redacted versions of confidential submissions may be filed via ECFS. Parties are advised that the FCC 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.

We exempt the proceeding initiated by this Notice from the FCC's *ex parte* rules.[4] This exemption serves the public interest by facilitating the full discussion of potentially sensitive matters. In the event the Commission were to take further action, any rule that the Commission were to propose would be subject to permit-but-disclose rulemaking procedures before it would be adopted, which would ensure the compilation of a full record.

For further information, contact Robert Finley, Attorney, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-7835, robert.finley@fcc.gov; or Ahmed Lahjouji, Engineer, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2061, ahmed.lahjouji@fcc.gov.

-FCC-

[4] 47 C.F.R. §§ 1.1200(a).