Before the

Federal Communications Commission

In the Matter of:

Public Safety and Homeland Security Bureau Requests Comment on Implementation of Measures to Prevent Location Tracking via the Diameter and Signaling System 7 Security Protocols

PS Docket No. 18-99

Request for Comment

Comment of

Electronic Privacy Information Center (EPIC)

May 28, 2024

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

I. Introduction

The **Electronic Privacy Information Center (EPIC)**[1] submits these comments to the Federal Communications Commission (FCC or Commission) regarding the Public Safety and Homeland Security Bureau's (Bureau's) request for comment on communications service providers' implementation of security countermeasures to prevent exploitation of vulnerabilities in the Signaling System 7 (SS7) and Diameter protocols.[2]

Significant weaknesses in SS7 have been known for more than a decade, including the ability to determine the physical location of a device, to disrupt phone service, to intercept or block text messages, and to redirect or eavesdrop on voice conversations.[3] Research has shown that these SS7 vulnerabilities can be present even where networks have been upgraded, as devices can switch to older network protocols when making phone calls or during SMS transmission.[4] By one 2018 estimate, nine out of ten SMS messages were able to be intercepted.[5] The ability to intercept and redirect messages exposes users to potential fraud, infiltration, and other forms of illicit monitoring that are not easily traceable. Unlike a SIM swap attack in which the victim loses service on their device,[6] in a redirect attack, the subscriber may not even be aware that their incoming messages are going to someone else.[7]

Hackers and members of the fast-growing surveillance-for-hire industry have developed new surveillance tools exploiting SS7 vulnerabilities to conduct espionage,[8] and enable fraud and identity theft targeting companies and their customers.[9] These surveillance-for-hire tools have

---

[1] EPIC is a public interest research center in Washington, DC seeking to protect privacy, freedom of expression, and democratic values in the information age.

[2] Public Safety and Homeland Security Bureau Requests Comment on Implementation of Measures to Prevent Location Tracking via The Diameter and Signaling System 7 Security Protocols, Request for Comment, DA 24-308 (Rel. Mar. 27, 2024), https://docs.fcc.gov/public/attachments/DA-24-308A1.pdf [hereinafter RFC].

[3] *See* Dep't of Homeland Security, *Study on Mobile Device Security* 53 (2017), https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf.

[4] *See* Positive Technologies, *Next-Generation Networks, Next-Level Cybersecurity Problems* 3 (2017), https://www.ptsecurity.com/upload/iblock/a8e/diameter_research.pdf; Positive Technologies, *Diameter Vulnerabilities Exposure Report* 6-7 (2018), https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf [hereinafter "Diameter Vulnerabilities Exposure Report"].

[5] *See* Diameter Vulnerabilities Exposure Report at 7.

[6] *See in re Protecting Consumers from SIM Swap and Port-Out Fraud*, Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 21-341 at ¶ 1 (Rel. Nov. 16, 2023), https://docs.fcc.gov/public/attachments/FCC-23-95A1.pdf (describing how a bad actor transfers the victim's service to a device in the bad actor's possession in a SIM swap attack).

[7] *See* Mitchell Clark, *Companies can silently reroute your texts to hackers, sometimes for just $16*, The Verge (Mar. 15, 2021), https://www.theverge.com/2021/3/15/22332315/sms-redirect-flaw-exploit-text-message-hijacking-hacking.

[8] *See* Kim Zetter, *The Critical Hole at the Heart of Our Cell Phone Networks*, Wired (Apr. 28, 2016), https://www.wired.com/2016/04/the-critical-hole-at-the-heart-of-cell-phone-infrastructure/.

[9] *See* Joseph Cox, *Criminals Are Tapping into the Phone Network Backbone to Empty Bank Accounts*, Motherboard (Jan. 31, 2019), https://www.vice.com/en/article/mbzvxv/criminals-hackers-ss7-uk-banks-metro-bank.

also been used to monitor and track journalists, activists, and dissidents.[10] There is reason to believe America's communications systems are being exploited in a systematic way by cybercrime-as-a-service operations.[11]

Members of Congress have repeatedly called for investigations into these vulnerabilities and for the development and implementation of stronger protocols to protect telephone subscribers.[12] There has also been growing media scrutiny of SS7 and of other security deficiencies in our nation's communications infrastructure.[13] Vulnerabilities seem to persist and to persist in being exploited, regardless of whether there has been widespread adoption of Communications Security, Reliability, and Interoperability Council (CSRIC) recommendations

[10] *See, e.g.*, Zack Whittaker, *Saudi spies tracked phones using flaws the FCC failed to fix for years*, TechCrunch (Mar. 29, 2020), https://techcrunch.com/2020/03/29/saudi-spies-ss7-phone-tracking/.

[11] *See* Russell Brandom, *For $500, this site promises the power to track a phone and intercept its texts*, The Verge (Jun. 13, 2017), https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime; *Study on Mobile Device Security supra* note 3 at 76-77 ("[the National Coordinating Center for Communications] believes many organizations appear to be sharing or selling expertise and services that could be used to spy on Americans").

[12] *See, e.g.*, Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era: Hearing Before the Subcomm. on Commc'ns and Tech. (Jan. 9, 2024), https://energycommerce.house.gov/events/communications-and-technology-subcommittee-hearing-safeguarding-americans-communications-strengthening-cybersecurity-in-a-digital-era [hereinafter "Safeguarding Americans' Communications"]; RFC at 4 n. 21 (citing to Letter from Ron Wyden, U.S. Senator, to Joseph Biden, President of the United States (Feb. 29, 2024), https://www.wyden.senate.gov/imo/media/doc/wyden-phone-hacking-letter-to-president-biden.pdf [hereinafter "2024 Wyden Letter"], Letter from Ron Wyden, U.S. Senator, and Ted Lieu, U.S. Representative, to Ajit Pai, Chairman, FCC (Mar. 28, 2017), Letter from Ron Wyden, U.S. Senator to Ajit Pai, Chairman, FCC (May 29, 2018)); Letter from T-Mobile to Sen. Ron Wyden in response to Sept. 14, 2017 letter (Oct. 13, 2017), https://www.wyden.senate.gov/imo/media/doc/10-13%20%20T%20Mobile%20Response.pdf; *see also* In the News, *What is SS7 and is China Using it To Spy on Trump's Cell Phone?* (Oct. 25, 2018), https://lieu.house.gov/media-center/in-the-news/what-ss7-and-china-using-it-spy-trump-s-cell-phone (reproducing Oct. 25, 2018 Motherboard article by Daniel Oberhaus); Samuel Gibbs, *US congressman calls for investigation into vulnerability that lets hackers spy on every phone*, The Guardian (Apr. 19, 2016), https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping.

[13] *See* Ryan Gallagher, *Senator Demands Overhaul of Telecom Security to Curb Abuses*, Bloomberg (Feb. 29, 2024), https://www.bloomberg.com/news/articles/2024-02-29/senator-demands-overhaul-of-telecom-security-to-curb-abuses; Mark Mazzetti, Ronen Bergman, and Adam Goldman, *Who Paid for a Mysterious Spy Tool? The F.B.I., an F.B.I. Inquiry Found.*, N.Y. Times (July 31, 2023), https://www.nytimes.com/2023/07/31/us/politics/nso-spy-tool-landmark-fbi.html (reporting on NSO spyware tool); Jan Haglund, *5G Is A Network Security Threat Wake-Up Call For Operators and Regulators*, Forbes (May 2, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/05/02/5g-is-a-network-security-threat-wake-up-call-for-operators-and-regulators/?sh=446c6a6f3e2f; Clark *supra* note 7; Thomas Brewster, *This Surveillance Tool Can Find You With Just Your Telephone Number—Did These 25 Countries Just Buy It?*, Forbes (Dec. 1, 2020), https://www.forbes.com/sites/thomasbrewster/2020/12/01/this-spy-tool-can-find-you-with-just-a-telephone-number-and-25-countries-own-it-warn-researchers/?sh=57d56fb331ed.

since 2020.[14] Discouragingly, the Cybersecurity and Infrastructure Security Agency (CISA) has still not published its unclassified 2022 report on SS7 surveillance and the security of America's communications networks.[15] EPIC sought access to this report earlier this year via a Freedom of Information Act (FOIA) request but has not yet received a copy.[16]

One comment filed in this docket,[17] attributed to a CISA whistleblower,[18] discusses incidents as recently as 2022. He said that:

> I have seen what appears to be reliable information related to numerous other exploits based on SS7 and Diameter that go beyond location tracking. Some of these involve issues like (1) the monitoring of voice and text messages, (2) the delivery of spyware to targeted devices, and (3) the influencing of U.S. voters by overseas countries using text messages./ Much more could be said, but this ends my public comments.[19]

This same CISA official has also called attention to vulnerabilities in SS7 and Diameter in the context of 5G security and Chinese espionage operations.[20]

Lawmakers and others have also highlighted the need to address these vulnerabilities. Sen. Ron Wyden recently emphasized in a letter to President Biden that this state of insecurity persists because the U.S. government has failed to set minimum cybersecurity requirements for wireless carriers, despite multiple federal agencies being aware of the threat.[21] The White

---

[14] *See* RFC at 4 (citing to Press Release, Chairman Ajit Pai, FCC, Chairman Pai Announces Industry Progress in Addressing Diameter Network Security Issue (Jul. 27, 2020), https://www.fcc.gov/document/pai-announces-industry-progress-addressing-diameter-security-issue).

[15] *See* 2024 Wyden Letter at 2.

[16] EPIC submitted its FOIA request on March 12, 2024, followed up on April 11, and followed up again on May 21. The most recent status, May 22, 2024, was "tasked to a program officer for record search."

[17] *See* Comment of Kevin Briggs, PSHSB 18-99 (Apr. 29, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10427582404839.

[18] *See, e.g.*, *It is dangerously easy to hack the world's phones*, The Economist (May 17, 2024), https://www.economist.com/science-and-technology/2024/05/17/it-is-dangerously-easy-to-hack-the-worlds-phones; Joseph Cox, *Cyber Official Speaks Out, Reveals Mobile Network Attacks in U.S.*, 404 Media (May 16, 2024), https://www.404media.co/email/79f7367c-bd3c-4bff-ac9f-85c738d08bec/.

[19] Comment of Briggs *supra* note 17 at 2.

[20] *See* Cox *supra* note 18.

[21] *See* 2024 Wyden Letter at 1-2; *see also* Christian Peeters, et al., *SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication*, 22 Procs ASIA CCS 2 (2022), https://dl.acm.org/doi/pdf/10.1145/3488932.3497756 (noting that NIST has publicly recommended that SMS no longer be used to deliver one time passwords); Communications Security, Reliability and Interoperability Council (CSRIC) VI: Working Group 3 Network Reliability and Security Risk Reduction, *Recommendations to Mitigate Security Risks for Diameter Networks* at 13 (Mar. 28, 2018), https://www.fcc.gov/sites/default/files/csric6report_recommendationstomitigateriskdiamterprotocol032018.pdf. Similar vulnerabilities may exist in the session initiation protocol (SIP), *see, e.g.*, CSRIC VII: Working Group 6 SIP Security Vulnerabilities, *Report on Session Initiation Protocol Security Challenges and Mitigation* at 22-47 (Mar. 10, 2021), *available at* https://www.fcc.gov/file/20609/download, *also available at* https://www.fcc.gov/CSRICReports.

House[22] and Congress[23] have each recognized the urgency of securing our nation's communications infrastructure.

With multiple recent, high-profile compromises of our communications' network, the Bureau's inquiry is urgently needed to effectively address these glaring vulnerabilities.[24]

II. The persistent threat to subscriber privacy and national security posed by our nation's communications network demands the Commission's attention.

To respond to the Bureau's explicit questions directly and unequivocally: the record suggests that these vulnerabilities persist and have been successfully exploited since 2018, and the Commission should investigate the extent of the problem and how to remedy it immediately, imposing mandatory reporting and audits as necessary.

The Bureau asks whether there have been "successful, unauthorized attempts to access the network user location data of communications service providers" since CSRIC VI's adoption of best practices in 2018.[25] Commentary in the record suggests the answer is yes.[26] The Bureau asks whether "communications service providers conveyed global titles to entities outside of the United States."[27] Again, commentary in the record suggests yes.[28]

The Bureau asks how the Commission can have greater visibility into the steps being taken to mitigate these vulnerabilities, and greater confidence that these steps are effective,[29] as well as how the Commission can have greater visibility into the conveyance of global titles.[30] The answer is mandatory reporting and auditing.

---

[22] *See, e.g.*, The White House, *National Cybersecurity Strategy Implementation Plan* 12-20 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf; "Critical Infrastructure Sectors", Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[23] *See, e.g.*, Safeguarding Americans' Communications *supra* note 12; Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

[24] *See, e.g.*, SECGov X Account, U.S. Securities and Exchange Comm'n (modified Jan. 24, 2024), https://www.sec.gov/secgov-x-account; Courtney Kube and Carol E. Lee, *U.S. intelligence officials determined the Chinese spy balloon used a U.S. internet provider to communicate*, NBC News (Dec. 28, 2023), https://www.nbcnews.com/news/investigations/us-intelligence-officials-determined-chinese-spy-balloon-used-us-inter-rcna131150; Cyber Safety Review Board, *Review of the Attacks Associated with Lapsus$ and Related Threat Groups* 48 (July 24, 2023), https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf.

[25] RFC at 4.

[26] *See* Comment of Briggs *supra* note 17 at 1. Tech reporting also suggests yes. *See, e.g.*, Whittaker *supra* note 10.

[27] RFC at 6.

[28] *See* Comment of Briggs at 1.

[29] *See* RFC at 5.

[30] *See id.* at 6.

III. The Commission should take a leadership role in securing our communications networks, including by auditing.

There are several immediate steps the Bureau and the Commission can and should take to better secure our communications networks. These include:

- requesting the unclassified CISA report referenced in Senator Wyden's letter and publishing it;
- articulating the Commission's authorities to address these vulnerabilities;
- commencing audits and investigations of carriers' practices to mitigate these vulnerabilities and to effectively detect unauthorized access to their networks; and
- (only if the Commission does not believe it has the authority to enact these recommendations) immediately requesting Congressional action to empower the agency to shore up the security of our communications networks.

The Bureau should request and publish the unclassified expert report on SS7 commissioned by CISA in 2022. Senator Wyden noted in his letter to President Biden that

> In addition to not taking responsibility for this problem, CISA is actively hiding information about it from the American people. The agency commissioned an independent expert report on this topic in 2022 which it permitted my staff to read at CISA's office in the fall of 2023. CISA refuses to publicly release this unclassified report, which includes details that are relevant to policymakers and Americans who care about the security of their phones.[31]

If the Bureau intends to shed greater light onto this problem, it should obtain and publicly release a copy of this unclassified report.

The Commission should articulate its authorities to address this problem. As Senator Wyden explained in his letter, part of the problem is that no agency has taken responsibility for fixing these vulnerabilities.[32] We observe that the Commission has authority under Section 201(b) of the Federal Communications Act to prohibit unjust and unreasonable practices, which it has invoked in data security contexts before.[33] Carriers are also bound under Section 222 to safeguard subscriber data, including but not limited to Customer Proprietary Network

---

[31] 2024 Wyden letter at 2.

[32] *See id.*

[33] *See, e.g.*, Comments of EPIC, *In re Data Breach Reporting Requirements*, WC Docket No. 22-21 at 7 (Feb. 22, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10222069458527 (citing to *in re TerraCom Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, File No.: EB-TCD-13-00009175, at ¶ 12 (Oct. 24, 2014), https://docs.fcc.gov/public/attachments/FCC-14-173A1.pdf). On multiple occasions Commissioner Starks has emphasized privacy and data security in matters grounded in the Commission's 201(b) authority. *See, e.g.*, Reply Comments of EPIC, *In re Review of International Section 214 Authorizations to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks*, IB Dkt. No. 23-119 at 14 (Oct. 2, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10020478023650 (citing to *In re Protecting Against Natl. Sec. Threats to the Commun. Supply Chain Through Fcc Programs*, 35 F.C.C. Rcd. 7821 (F.C.C. 2020) ("untrustworthy equipment that threatens our data privacy and network security cannot be managed or tolerated in any form") and to *In re Protecting Against Natl. Sec. Threats to the Commun. Supply Chain Through Fcc Programs Huawei Designation Zte Designation*, 34 F.C.C. Rcd. 11423 (F.C.C. 2019) ("…I have said many times that the untrustworthy equipment from these companies could readily serve as a 'front door' for Chinese intelligence gathering, at the expense of our privacy and national security.")).

Information (CPNI).[34] Additionally, unauthorized access to location data can pose serious threats to the personal safety of survivors of domestic violence, providing the Commission with relevant authority under its "safety of life" charge.[35]

The Commission should also commence audits and investigations of carriers' practices. The contrast both amongst their filings, and between their filings and the CISA whistleblower's, are cause for concern. Per their own filings, Verizon and T-Mobile both indicated that they are unaware of any issues since 2018.[36] T-Mobile goes further and says it does not want to share audit data with the Commission.[37] Verizon indicated that it shared confidential information with the Commission in October 2022.[38] AT&T indicated that it "shared specific, confidential information concerning our knowledge of known threats to SS7 and the specific actions AT&T is taking (and plans to take) to address those threats."[39] CTIA indicated that to the extent SS7 or Diameter protocols are still being used, CSRIC safeguards are in place,[40] which, even if true, does not address whether vulnerabilities in our communications networks are still being exploited.

CTIA also argues that any audit requirement would complicate the "existing patchwork" of audit-related regulations and "would be in tension with the Administration's goal to harmonize cybersecurity requirements."[41] The urgency of currently compromised communications security supersedes any fears of future regulatory burden on companies. If providers believe their existing audits are adequate to assist the Commission in remedying these vulnerabilities, companies should furnish those audits to the Commission immediately and without reservation, and let the Commission decide whether or not existing regulations are adequate to ensure the persistent security of our nation's communications networks.

---

[34] *See, e.g.*, Fed. Commc'ns Comm'n, *In re Data Breach Reporting Requirements*, Report & Order, WC Docket No. 22-21 at ¶ 15-20 (Rel. Dec. 21, 2023), https://docs.fcc.gov/public/attachments/FCC-23-111A1.pdf; Reply Comments of EPIC, et. al., *In re Data Breach Reporting Requirements*, WC Docket No. 22-21 at 11-12 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814; Reply Comments of EPIC, National Consumer Law Center, et. al., *In re Protecting Consumers from SIM-Swap and Port-Out Fraud*, WC Dkt. No. 21-341 at 6, 19-22 (Feb. 12, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10213160552872.

[35] *See, e.g.*, Comment of EPIC and Public Knowledge, *In re Supporting Survivors of Domestic and Sexual Violence*, WC Dkt. No. 22-238 at 25-26 (May 23, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/105242630421222.

[36] *See* Comment of Verizon, PSHSB 18-99 at 1 (Apr. 26, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/104260196006694; Comment of T-Mobile USA, Inc., PSHSB 18-99 at 4 (Apr. 26, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10426217320614.

[37] *See* Comment of T-Mobile USA, Inc. at 7 ("Providers should not be required to disclose internal and third party security audits to the Commission, including the frequency and results, and documentation pertaining to them.").

[38] *See* Comment of Verizon at 2.

[39] Comment of AT&T Services, Inc., PSHSB 18-99 at 3 (Apr. 26, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10426568605710.

[40] *See* Comment of CTIA, PSHSB 18-99 at 12 (Apr. 26, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10426291025512 ("Finally, neither SS7 nor its successor Diameter are widely used to deliver SMS messages on U.S. networks.").

[41] *Id.* at 23.

The Commission can immediately act upon these recommendations using its authorities under Title II. However, if the Bureau is concerned that the Commission's existing authorities are not sufficient to defend our nation's communications networks, it should articulate why and immediately request Congressional action to remedy that deficiency.

IV. Conclusion

We appreciate the opportunity to support the Commission in strengthening the security of our communications networks.

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036