epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

BY EMAIL
Email: foia@hq.dhs.gov

March 12, 2024

Mason Clutter
Chief Privacy Officer/Chief FOIA Officer
The Privacy Office
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Ave SE
STOP-0655
Washington, D.C. 20528-0655

Dear Ms. Clutter,

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Homeland Security ("DHS").

EPIC requests the unclassified 2022 report, including any appendices or other attachments, by independent experts that the Cybersecurity and Infrastructure Security Agency (CISA) commissioned on the threat posed by surveillance technology exploitation of flaws in Diameter and Signaling System 7 (SS7).[1] This report is essential to adequately secure our country's communications networks, a vital component of our critical infrastructure cybersecurity. With multiple recent, high-profile compromises of our communications' network, this information is urgently needed to effectively address these glaring vulnerabilities.[2]

Background

Signaling System 7 (SS7) is a global standard signaling protocol used for telecommunications traffic for most of the world's Public Switched Telephone Network (PSTN) calls.[3] Significant weaknesses in SS7 have been known for more than a decade, including the ability

[1] *See* Letter from Ron Wyden, U.S. Sen., to Joseph R. Biden, Jr., President of the United States (Feb. 29, 2024), https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/r.DSbwvU6XD4/v0 [hereinafter Wyden SS7 Letter].
[2] *See, e.g.*, SEC, *SECGov X Account*, https://www.sec.gov/secgov-x-account (last modified Jan. 24, 2024); Courtney Kube & 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 Rev. Bd., *Review of the Attacks Associated with Lapsus$ and Related Threat Groups* (July 24, 2023), https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf.
[3] DHS Sci. & Tech. Directorate, *Study on Mobile Device Security* 53 (Apr. 2017), https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf.

to determine the physical location of the device, disrupt phone service, intercept or block text messages, and redirect or eavesdrop on voice conversations.[4] This is likely true even where networks have been upgraded, as devices will often switch to older network protocols when making phone calls or during SMS transmission.[5] By one estimate, nine out of ten SMS messages were able to be intercepted.[6] There is reason to believe SS7 is being exploited in a systematic way by cybercrime-as-a-service operations.[7] However, despite the urgency of these threats and increasing public attention to SS7 vulnerabilities, Sen. Ron Wyden—in a February 29 letter to President Joe Biden—noted that no agency has taken responsibility for this problem.[8] The Administration[9] and Congress[10] have each recognized the urgency of securing our nation's communications infrastructure.

CISA is the entity charged with leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.[11] This includes coordinating information sharing groups,[12] publishing known vulnerabilities,[13] publishing best practice guidance,[14] and supporting and directing expert studies on cybercrime tactics that target communications infrastructure.[15]

Sen. Wyden's letter also revealed that, in 2022, CISA had commissioned an unclassified "independent expert report" on the serious threat of SS7 surveillance, and that this report was complete as of the fall of 2023.[16] However, CISA has thus far refused to publicly release the unclassified report, "which includes details that are relevant to policymakers and Americans who

---

[4] *Id.*
[5] Positive Techs., *Next-Generation Networks, Next-Level Cybersecurity Problems* 3 (2017), https://www.ptsecurity.com/upload/iblock/a8e/diameter_research.pdf; Positive Techs., Diameter Vulnerabilities Exposure Report 6–7 (2018), https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf.
[6] Diameter Vulnerabilities Exposure Report, *supra* note 5, at 7.
[7] Russell Brandon, *For $500, this site promises the power to track a phone and intercept its texts*, Verge (June 13, 2017), https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime; Study on Mobile Device Security, *supra* note 3, at 76–77 ("NCC believes many organizations appear to be sharing or selling expertise and services that could be used to spy on Americans").
[8] Wyden SS7 Letter, *supra* note 1, at 2.
[9] *See, e.g.*, White House, National Cybersecurity Strategy Implementation Plan 12–20 (July 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf; CISA, *Critical Infrastructure Sectors*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (last visited Mar. 12, 2024).
[10] *See, e.g.*, House Comm. on Energy & Com., *Chairs Rodgers and Latta Announce Subcommittee Hearing on Improving Cybersecurity for U.S. Communications Networks* (Jan. 4, 2024), https://energycommerce.house.gov/posts/chairs-rodgers-and-latta-announce-subcommittee-hearing-on-improving-cybersecurity-for-u-s-communications-networks; CISA, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia (last visited Mar. 12, 2024).
[11] CISA, *About CISA*, https://www.cisa.gov/about (last visited Mar. 12, 2024).
[12] *See, e.g.*, CISA, *Information Sharing*, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing (last visited Mar. 12, 2024).
[13] *See, e.g.*, CISA, *Coordinated Vulnerability Disclosure Process*, https://www.cisa.gov/coordinated-vulnerability-disclosure-process (last visited Mar. 12, 2024).
[14] *See, e.g.*, CISA, Secure by Design, https://www.cisa.gov/securebydesign (last visited Mar. 12, 2024).
[15] *See, e.g.*, *Review of the Attacks Associated with Lapsus$ and Related Threat Groups*, supra note 2.
[16] Wyden SS7 Letter, *supra* note 1, at 2.

care about the security of their phones."[17] This report is critical to understanding the threat and potential solutions and the public has a right to know.

Request for Expedited Processing

EPIC is entitled to expedited processing of this request under the FOIA.[18] Specifically, EPIC's request satisfies the agency regulation 6 C.F.R. § 5.5(e)(1)(ii) because it involves "[a]n urgency to inform the public about an actual or alleged federal government activity," and because the request is "made by a person who is primarily engaged in disseminating information."[19]

First, there is "an urgency to inform the public about an actual or alleged government activity."[20] Recent events create a patent "urgency to inform the public" about SS7 vulnerabilities, the government's response to these threats to Americans, and what the best path forward might be to resolving this problem. There is growing media scrutiny of SS7 and other infiltrations and exploitations of our nation's communications infrastructure.[21] Hackers and members of the fast-growing surveillance-for-hire industry have developed new surveillance tools exploiting SS7 vulnerabilities to conduct espionage;[22] enable fraud and identity theft targeting companies and their customers;[23] and track journalists, activists, and dissidents.[24] In response to these concerns, members of Congress have called for investigations into these vulnerabilities and fixes.[25] EPIC's request thus

---

[17] *Id.*
[18] 5 U.S.C. §§ 552(a)(6)(E)(i)(I), 552(a)(6)(E)(v)(II).
[19] 6 C.F.R. § 5.5(e)(1)(ii).
[20] *Id.*
[21] *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, & 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; Jan Häglund, *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; Mitchell Clark, *Companies can silently reroute your texts to hackers, sometimes for just $16*, Verge (Mar. 15, 2021), https://www.theverge.com/2021/3/15/22332315/sms-redirect-flaw-exploit-text-message-hijacking-hacking; Thomas Brewster, *This Surveillance Tool Can Find You With Just Your Telephone Number — Did These 25 Countries 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.
[22] *See, e.g.*, 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/.
[23] *See, e.g.*, 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.
[24] *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/.
[25] *See* Wyden SS7 Letter, *supra* note 1; Letter from Anthony Russo, Vice President, Fed. Leg. Affs., T-Mobile US, to Ron Wyden, U.S. Sen. (Oct. 13, 2017), https://www.wyden.senate.gov/imo/media/doc/10-13%20%20T%20Mobile%20Response.pdf; *see also* Daniel Oberhaus, *What is SS7 and is China Using It To Spy on Trump's Cell Phone?*, Motherboard (Oct. 25, 2018), https://www.vice.com/en/article/598xyb/what-is-

satisfies the first standard for expedited processing because there is an urgency to inform the public of the CISA expert report and recommendations relating to SS7.

Second, as the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA.[26] EPIC is a non-profit organization committed to privacy, open government, and civil liberties that consistently discloses documents obtained through FOIA on its website, EPIC.org, and its online newsletter, the *EPIC Alert*.[27]

In submitting this request for expedited processing, EPIC certifies that this explanation is true and correct to the best of its knowledge and belief.[28]

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes.[29] Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplications fees assessed.[30]

In addition, because EPIC's request satisfies each of the two alternative standards in 6 C.F.R. § 5.11(k) for granting a fee waiver, any duplication fees should also be waived.[31]

1. *Disclosure will contribute significantly to public understanding of the risks of insecure communications and how to improve cybersecurity in communications infrastructure.*

Disclosure of the CISA expert report on SS7 will contribute significantly to public understanding of cybercrime and foreign surveillance made possible by exploiting vulnerabilities in our communications infrastructure. In determining whether the disclosure will contribute to the public understanding, DHS considers: (i) whether the subject concerns identifiable operations or activities of the federal government; (ii) whether disclosure of the records is meaningfully informative in order to be "likely to contribute" to an increased public understanding of those operations or activities; (iii) whether the disclosure contributes to the understanding of a reasonably broad audience, as opposed to the individual understanding of the requester; and (iv) whether the public's understanding of the subject in question is enhanced by the disclosure to a significant extent.[32]

---

ss7-and-is-china-using-it-to-spy-on-trumps-cell-phone; Samuel Gibbs, *US congressman calls for investigation into vulnerability that lets hackers spy on every phone*, Guardian (Apr. 19, 2016), https://www.theguardian.com/technology/2016/apr/19/ss7-hack-us-congressman-calls-texts-location-snooping.

[26] 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

[27] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[28] 5 U.S.C. § 552(a)(6)(E)(vi); 6 C.F.R. §5.5(e)(3).

[29] *EPIC v. DOD*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

[30] 5 U.S.C. § 552(a)(4)(A)(ii)(II); 6 C.F.R. § 5.11(d)(1).

[31] 6 C.F.R. § 5.11(k); 5 U.S.C. § 552(a)(4)(A)(iii).

[32] 6 C.F.R. § 5.11(k)(2).

First, EPIC's request concerns "identifiable operations or activities" of the federal government, namely those of CISA.[33] As noted above, CISA is the entity charged with leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.[34]

Second, public disclosure of this report will be meaningfully informative and "likely to contribute" to increased public understanding of both the threats and possible policy remedies. There is currently no public information about this report, and CISA is uniquely situated as the national coordinator for critical infrastructure security to share its expertise on this urgent issue. Disclosure of this report will provide the public with a better and more comprehensive understanding of the nature of SS7 and other communications network vulnerabilities as well as how to mitigate them. The report that EPIC requests is expected to shed new light on the persistent severity of the problem and on promising solutions that will be meaningfully informative for strengthening our nation's cybersecurity posture.

Third, EPIC's request will contribute to the understanding of a reasonably broad audience. Under 6 C.F.R. § 5.11(k)(2)(iii), "it shall be presumed that a representative of the news media will satisfy this consideration."[35] As mentioned above, EPIC is a "representative of the news media."[36] EPIC routinely publishes records from its FOIA requests on its website, epic.org, and EPIC's FOIA work is frequently covered by news outlets.[37]

Fourth, the disclosure will significantly enhance the public's understanding of the activity. The expert report from 2022 has not yet been publicly released by CISA.[38] Release of this report will publicize previously inaccessible information about the cybersecurity of our communications network from the agency tasked with leading the national effort to understand and reduce risk to our cyber infrastructure.[39]

2. *Disclosure is not primarily in the commercial interest because EPIC is a nonprofit seeking this information for public education.*

Disclosure of the requested information is "not primarily in the commercial interest" of EPIC.[40] DHS considers two factors to determine whether this is met: (i) whether there is "any commercial interest of the requester . . . that would be furthered by the requested disclosure"; and (ii) whether "the public interest is greater than any identified commercial interest in disclosure."[41] Again, EPIC is a non-profit organization committed to privacy, open government, and civil liberties.[42] EPIC intends to use this information for public education, often publishing records obtained through the

[33] 6 C.F.R. § 5.11(k)(2)(i).
[34] CISA, *About CISA*, https://www.cisa.gov/about (last visited Mar. 12, 2024).
[35] 6 C.F.R. § 5.11(k)(2)(iii).
[36] 6 C.F.R. § 5.11(k)(2)(iii); EPIC v. Dep't of Def., 241 F. Supp. 2d 5, 15 (D.D.C. 2003).
[37] *See* EPIC, *EPIC in the News*, https://epic.org/news/epic_in_news.php/.
[38] Wyden SS7 Letter, *supra* note 1, at 2.
[39] CISA, About CISA, https://www.cisa.gov/about (last visited Mar. 12, 2024).
[40] 6 C.F.R. § 5.11(k)(3).
[41] *Id.*
[42] *See* EPIC, *supra* note 27.

FOIA on its website EPIC.org. Further, as demonstrated above, EPIC is a news media requester and satisfies the public interest standard under agency regulations.[43]

For these reasons, EPIC's request for a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. EPIC anticipates your determination on our request within ten calendar days per 5 U.S.C. § 552(a)(6)(E)(ii)(I). Please send any responsive documents via email to FOIA@epic.org cc: jscott@epic.org in searchable PDF form. For questions and correspondence regarding this request contact Jeramie Scott at FOIA@epic.org cc: jscott@epic.org.

Respectfully Submitted,

/s Jeramie Scott
Jeramie Scott
Senior Counsel
Director, Project on Surveillance Oversight

/s Chris Frascella
Chris Frascella
EPIC Counsel

/s Chris Baumohl
Chris Baumohl
EPIC Law Fellow

[43] *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).