FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Facilitating Implementation of Next Generation 911 Services (NG911)	)	PS Docket No. 21-479
	)	

Relating to the
Notice of Proposed Rulemaking
Issued June 9, 2023

Comments of

Electronic Privacy Information Center

August 9, 2023

By:
Chris Frascella
Law Fellow
frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

Table of Contents

Comments

I. Introduction and Summary

The **Electronic Privacy Information Center (EPIC)** files these comments on the Notice of Proposed Rulemaking (NPRM) regarding "Facilitating Implementation of Next Generation 911 Services (NG911)" issued on June 9, 2023.[1] We urge the Commission to recognize the sensitive nature of NG911 data, to require cybersecurity maturity assessments as part of readiness testing (building upon the foundations outlined by CSRIC, CISA, and others), and to address privacy issues such as misuse of NG911 data.

II. The Commission should put greater emphasis on safeguarding NG911 data.

As we noted in the Commission's rulemaking on location-based routing, creating new troves of sensitive data (such as precise location data) is dangerous without first ensuring that that data will be safeguarded.[2] At a 2018 NIST workshop on Public Safety Mobile Application Security, mostly focused on apps used by first responders, discussants emphasized that the confidentiality, integrity, and availability of data related to emergency services, especially location information, is critical.[3] This is especially salient in light of recent Congressional inquiry into the security of FirstNet.[4]

The Commission should apply these same priorities to the NG911 context. The Commission has voiced its enthusiasm about new types of transmissible data including text, photos,

---

[1] *In re* Facilitating Implementation of Next Generation 911 Services (NG911), Notice of Proposed Rulemaking, PS Docket No. 21-479 (Rel. June 9, 2023, available at https://docs.fcc.gov/public/attachments/FCC-23-47A1.pdf [hereinafter NPRM]. The Proposed Rule was published in the Federal Register at 88 Fed. Reg. 43,514 (July 10, 2023) and is available at https://www.federalregister.gov/documents/2023/07/10/2023-14402/facilitating-implementation-of-next-generation-911-services-ng911#footnote-25-p43518.

[2] See Comments of EPIC, *In re* Location-Based Routing for Wireless 911 Calls, PS Docket No. 18-64 (Feb. 16, 2023), available at https://www.fcc.gov/ecfs/search/search-filings/filing/10216148603009 [hereinafter EPIC LBR Comments].

[3] See NIST, Public Safety Mobile Application Security Requirements Workshop Summary, NISTIR 8018 at 10 (Jan. 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf.

[4] See, e.g., Press Release, Wyden Requests Annual Cybersecurity Audits of Phone Network for First Responders and Military Personnel (Apr. 12, 2023), https://www.wyden.senate.gov/news/press-releases/wyden-requests-annual-cybersecurity-audits-of-phone-network-for-first-responders-and-military-personnel-.

and videos.[5] National security writers have rightly characterized this as an increased attack surface.[6] One of the Commission's advisory bodies, the Communications Security, Reliability and Interoperability Council (CSRIC), made similar observations in September 2020, noting that Emergency Communications Centers' Records Management Systems are often shared with multiple agencies and that those that are internet-connected or delivered via the cloud "now have a broader set of attack vectors than ever."[7] However, despite this and despite DHS noting the attractiveness of NG911 data to bad actors,[8] the Commission has not placed a similar emphasis on the importance of safeguarding this data in this rulemaking. To correct this, we offer the Commission the following recommendations.

III. The Commission should require improved cybersecurity practices, assessed as part of a readiness determination.

We support the Commission's proposed definition of NG911 which includes an emphasis on security.[9] Meeting basic cybersecurity standards should be an element in a readiness determination.[10]

---

[5] See e.g., NPRM at ¶ 10; Statement of Chairwoman Jessica Rosenworcel, *In re* Facilitating Implementation of Next Generation 911 Services (June 8, 2023), https://docs.fcc.gov/public/attachments/FCC-23-47A2.pdf.
[6] See, e.g., Mark Grzegorzewski and William Holden, 911? We Have an Emergency: Cyberattacks On Emergency Response Systems, Lawfare (May 3, 2023), https://www.lawfaremedia.org/article/911-we-have-an-emergency-cyberattacks-on-emergency-response-systems.
[7] See Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG 9-1-1 Implementations, Communications Security, Reliability, and Interoperability Council VII (CSRIC VII) at 41 (Sept. 16, 2020), available at https://www.fcc.gov/media/107106 [hereinafter CSRIC Sept. 2020].
[8] See, e.g., Cyber Risks to Next Generation 911, Dept. Homeland Security Office of Emergency Communication at 1, available at https://www.911.gov/assets/Cyber-Risks-to-Next-Generation-911.pdf (last accessed Aug. 9, 2023) ("location-based records and databases that support NG911 are of interest to cyber criminals, data miners, and even nation-states wanting to access and exploit that information").
[9] See NPRM at ¶ 51 (sharing definition from Spectrum Auction Reauthorization Act of 2023 which includes that the IP-based system be secure; "We note that recent legislative definitions include qualitative descriptors of NG911 systems, such as security, interoperability, and use of commonly accepted standards, as well as specific technical capabilities. Should we include any or all of these elements in a definition of NG911 adopted by the Commission?").
[10] See NPRM at ¶ 43 (e.g. proposing that "IP-capable" or "NG911-capable" be part of a readiness determination).

In its March 2021 report, CSRIC noted that there are inherent risks in the transition to NG911.[11] Similarly, in 2016, the Task Force on Optimal PSAP Architecture (TFOPA) noted that apps interfacing with PSAPs need to be subject to more rigorous requirements and safeguards.[12]

CSRIC called for the Commission to include cybersecurity maturity as a question in annual Fee Reports.[13] It also highlighted the risks implicit in new functionality being deployed too quickly:

> The communications technology required to support the NG9-1-1 infrastructure is adding new hardware elements and software functionality at an unprecedented pace, including many features that address existing security threat vectors and/or secure known vulnerabilities. However, with each new addition comes the high probability that a new cyber threat is also enabled. In some cases, this includes the very features originally implemented to secure the NG9-1-1 system in the first place.[14]

CSRIC proposed that agencies implement several methods including but not limited to: continuous monitoring, vulnerability assessments every 90 days, multiple backups (in the event of a ransomware encryption attack, for example), having a written cyber response plan tested quarterly, using network segmentation and putting sensitive information behind additional firewalls, implementing a least-privileged access model, cyber-hygiene training, and implementing additional protections for remote access.[15] CSRIC recommended that the Commission collect information about cybersecurity maturity from the 9-1-1 community[16] and consider referencing existing models or frameworks such as those from NIST, CIS, and CMMC.[17] And there are still other resources readily available which the Commission could draw from in securing NG911 systems.[18] This

---

[11] See CSRIC VII Report Measuring Risk Magnitude and Remediation Cost in 911 and NG911 Networks at 19 (Mar. 10, 2021), available at https://www.fcc.gov/file/20607/download [hereinafter CSRIC March 2021] (citing to *Quantifying Systemic Cyber Risk*).
[12] See Task Force on Optimal PSAP Architecture, Optimal Cybersecurity Approach for PSAPs Final Report at 19 (Dec. 2015), https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf (Point 4.2).
[13] See CSRIC March 2021 at 23.
[14] Id. at 24.
[15] See id. at 25-27.
[16] See id. at 42-43.
[17] See id. at 33-40, 41-42.
[18] See, e.g., Cybersecurity and Infrastructure Security Agency, Cyber Risks to Next Generation 9-1-1, SAFECOM/NCSWIC (Nov. 2019) https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf.

includes explicit use cases outlined by CSRIC, such as an employee being fooled by social engineering[19]—a phenomenon likely to be supercharged by AI.[20]

Providers in this rulemaking have called for PSAP readiness testing.[21] We urge the Commission to include standardized cybersecurity maturity assessments as part of this testing.

IV. The Commission must also address privacy, not merely cybersecurity.

Security protects against unauthorized access, but the Commission should not overlook the threat of internal, authorized misuse as well. As we noted in our comments on location-based routing, emergency location data has been misused by carriers in the past.[22] The Commission should articulate clear guidelines for how NG911 data is to be used and by whom, what uses are prohibited, and what expectations the Commission has about data minimization, which includes limits on both collection and retention.[23]

V. Conclusion

We appreciate the Commission's efforts to improve our nation's emergency response system, however we urge greater emphasis on protecting the new forms of data that will power that system.

Respectfully submitted, August 9, 2023.

Chris Frascella
Law Fellow
frascella@epic.org
Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, D.C. 20036

[19] See CSRIC Sept. 2020 at 43-44.
[20] See, e.g., Alessandro Mascellino, Dark Web Markets Offer New FraudGPT AI Tool, Infosecurity Magazine (July 26, 2023), https://www.infosecurity-magazine.com/news/dark-web-markets-fraudgpt-ai-tool.
[21] See, e.g., NPRM at ¶ 42 (Verizon calling for PSAP readiness standard, NPRM referring to T-Mobile calling for comprehensive testing).
[22] See EPIC LBR Comments at 2-4.
[23] See, e.g., id. at 7-9.