**Communications Security, Reliability, and Interoperability Council IX**

**Tasks and Working Groups**

June 2024

**Working Group 1: Harnessing Artificial Intelligence/Machine Learning to Ensure the Security, Reliability, and Integrity of the Nation’s Communications Networks**

*Co-chairs: Vijay Gurbani, Vail Systems, and Jason Hogg, Microsoft*

*FCC Liaison:**Zenji Nakazawa*

The Chairwoman of the FCC directs CSRIC IX to provide recommendations on how to leverage artificial intelligence and machine learning (AI/ML) to enhance the confidentiality, integrity, and availability of communications networks and to recommend how policies or programs can be developed or leveraged to ensure that AI/ML is used in a nondiscriminatory, transparent, and socially responsible way. This effort follows ongoing efforts by the White House to advance a cohesive and comprehensive approach to AI-related risks and opportunities.[[1]](#footnote-2) Congress also recently held a hearing on May 16, 2023, concerning the need to regulate AI, among other things.[[2]](#footnote-3) AI/ML and Data Driven Algorithms (DDA) are driving digital transformation to create value in all facets of our modern society from Main Street and Wall Street to Silicon Valley. AI is a branch of computer science[[3]](#footnote-4) that focuses on building and managing technology that can learn to autonomously make decisions and carry out actions on behalf of a human being. Another way to look at AI is simply as a field,[[4]](#footnote-5) which combines computer science and robust datasets, to enable problem-solving. But neither definition fully captures AI’s critical role in communications nor its sheer potential to influence, transform, and remake our digital world.

As the FCC’s Technical Advisory Committee (TAC)[[5]](#footnote-6) observed in December 2022, AI can provide real value when it comes to network optimization; it is already being increasingly applied to optimize, operate, and protect network services—and this trend is only going to increase. The TAC noted, for example, that AI is being incorporated in 5G chipsets to enhance 5G coverage and improve uplink performance. The TAC also noted that AI-assisted communication design can help navigate the complexity encountered by end users in a climate of increasing number of bands, channel bandwidths, and advanced antenna technologies. AI also serves a role in network security by evaluating vast amounts of data to support cybersecurity controls such as endpoint detection response, software update automation, and threat emulation.

But while AI is promising as a tool for optimizing and protecting communications networks, it could be used as yet another threat vector to network security. AI relies on data to feed its ability to learn, adapt, and evolve, and the decisions or outcomes produced by AI are only as reliable as the data it receives. A bad actor, for example, could manipulate datasets used by AI to control, subvert, or otherwise corrupt the dataset to cause the AI to deliver poor or false results.[[6]](#footnote-7) This injection of so-called “poisoned” or “polluted” data can lead to not only a loss of confidence in the software but also an opportunity for a bad actor to insert malicious code into software to create a backdoor to the target, similar to the SolarWinds intrusion.

CSRIC has never previously examined the security risks posed by AI. CSRIC IX will begin developing a comprehensive understanding of AI that will serve as a foundation for examining the benefits and challenges AI poses to the integrity of communications networks, and what policies or actions the FCC should consider to mitigate the harms posed by AI.

CSRIC IX will consider how AI/ML increases the threat attack surface and how best to mitigate such security challenges. CSRIC IX will consider how the FCC and industry can promote sound policies and practices that support public safety, network security, and resilience, while also preventing and mitigating harms associated with the use of AI. Specifically, CSRIC will consider current trends, developments, and related standards work in “hardening” AI, protecting data used for training, and identify gaps in efforts to develop AI’s cyber-readiness and trustworthiness, and how the FCC and industry can clarify and strengthen efforts on how AI is used to support and optimize communications networks, while promoting ethical innovation and investment. Finally, CSRIC IX will consider how to promote sound policies and practices in the use of AI applications specifically intended for the public safety communications environment (e.g., AI applications that focus on 911 or alerting) while also preventing and mitigating harms to the security, reliability, and integrity of public safety and emergency response networks.

*Milestones:*

1. Report on the Threats Posed by Artificial Intelligence/Machine Learning Systems to the Security, Reliability and Integrity of Networks and Recommendations on How to Overcome Them, **June 2025**
2. Report on Recommended Best Practices for the FCC and Industry on the Ethical and Practical Use of Artificial Intelligence/Machine Learning, **September 2025**
3. Report on Best Practices for the Use of Artificial Intelligence/Machine Learning Systems Specifically Intended for Public Safety Network, **March 2026**

**Working Group 2: Ensuring Consumer Access to 911 on All Available Networks As Technology Evolves**

*Co-chairs: Brandon L. Abley, NENA, and Stephen Hayes, Ericsson*

*FCC Liaisons: Gerald English and Ryan Hedgpeth*

The Chairwoman of the FCC directs CSRIC IX to provide recommendations regarding the impact, functionality, and potential limitations of the increasing number of “back-up” options available to consumers for calling 911. When consumers dial 911, seconds matter. It is imperative for 911 calls to be answered by someone who can send help fast and to the right location. The Commission has taken steps to improve 911 service to facilitate improved emergency response times. As technology evolves, consumers may use an increasingly wide range of wireless devices that have the capacity to transmit 911 calls over a variety of networks. For example, consumers’ existing wireless phones typically will attempt to use a home carrier’s network to transmit 911 calls, but when the home network is unavailable (e.g., due to lack coverage or a network outage), the device may have alternative options for connecting to 911, including another carrier’s network (with or without a roaming agreement), WiFi calling, or a satellite network. As back-up options become increasingly available, wireless devices that cannot make a 911 call on their primary network will need to be capable of “searching” sequentially for alternative options to successfully connect the call. In addition, industry is currently involved in the evolution of legacy 911 to Next Generation 911 (NG911). This evolution will represent a significant shift in how traffic is relayed to, and received by, Public Safety Answering Points (PSAPs) and in the type and quality of data available to the PSAP. These technological advances raise several questions, including:

* How should consumer devices prioritize the potential back-up network options for connecting to 911?
* What connection latency may be introduced by this alternative network “search” process? If the latency is extreme (more than 20 seconds), what measures can be taken to reduce the latency? Should device manufacturers or service providers develop “user prompts” to advise callers who experience significant latency that the phone is in the process of connecting to 911?
* What information will the PSAP, and the relevant functional elements associated with Next Generation Core Services, receive from a back-up, alternative network sources (e.g., dispatchable location, coordinate-based location, call-back number)? If the back-up network options degrade the information flow from the originating call to the PSAP, what can be done to ensure that actionable caller location and other essential data reliably reaches the PSAP to dispatch aid?
* Will there be relevant classes of service developed to identify the source type of the call for PSAPs? If not, what information can the PSAPs realistically expect to receive to help them quickly and accurately identify the source (WiFi, satellite, etc.) of the call?
* Are there any limitations to any of these back-up network sources (i.e. less granular location information, lack of automatic number identification (ANI)/automatic location identification (ALI), inability to perform location based routing)?
* What, if any, impact do the issues identified with alternative network options for connecting to 911 have on NG911 services and capabilities?
* Will the use of any of these alternative options impact the capabilities of, or information delivered to, PSAPs by NG911?

CSRIC IX will be tasked with looking holistically at the entire communications ecosystem, rather than any one individual platform. Matching consumer expectations with available technology is an ongoing concern, and CSRIC IX is directed to examine and provide recommendations on how to best ensure 911 connectivity, and functionality, across multiple platforms and options, including systems associated with NG911.

*Milestones:*

1. Report on Recommendations and Best Practices for Connecting Stalled 911 Calls Through Alternative Network Options, **June 2025**
* Identifying, prioritizing and quickly connecting 911 calls via alternative network options;
* Reducing latency when utilizing alternative network options and for ameliorating the impact of any significant latency that cannot be avoided;
* Reducing, or eliminating, any technical limitations currently in place for any, or all, alternate network options.
1. Report on Recommendations for Preventing Adverse Impacts on PSAPs and NG911 from 911 Calls Made Through Alternative Network Options, **March 2026**
* Providing PSAPs with actionable, accurate, information, including caller location and source (call type) of call when alternative network options are selected and utilized; and
* Addressing any impacts, positive or negative, that these alternative network options might have on NG911.

**Working Group 3: Preparing for 6G Security and Reliability**

*Co-chairs: Brian Daly, AT&T, and George Woodward, Rural Wireless Association*

*FCC Liaison: Jeffery Goldthorp*

The Chairwoman of the FCC directs CSRIC IX to examine and address security and reliability risks unique to emerging 6G networks and services. CSRIC IX will develop a plan for the development and deployment of reliable and security 6G networks and services that minimize privacy risks. 6G networks are at least seven years from commercial deployment, but wireless technology moves at such a brisk pace that the Commission is compelled to seek early recommendations from stakeholders that will lead to more secure and reliable 6G networks and services. 6G is expected to result in orders of magnitude improvements in network speed and latency, enabling capabilities that cause distinctions between the physical and cyber worlds to fade. CSRIC IX will make an early foray into examining and addressing potential security and reliability risks in emerging 6G networks and service.

*Milestones:*

1. Report on Potential Security and Reliability Risks in 6G and Recommendations for Mitigation, **December 2025**

1. Biden-⁠Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans’ Rights and Safety, Fact Sheet, May 4, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/. [↑](#footnote-ref-2)
2. Oversight of A.I.: Rules for Artificial Intelligence: Hearing Before the Subcomm. on Privacy, Technology, and the Law, 118th Cong. (2023), https://www.judiciary.senate.gov/committee-activity/hearings/oversight-of-ai-rules-for-artificial-intelligence; Oversight of A.I.: Rules for Artificial Intelligence, S.Hrg. 118-37, https://www.congress.gov/event/118th-congress/senate-event/LC71543/text?q=%7B%22search%22%3A%22Oversight+of+A.I.%3A+Rules+for+Artificial+Intelligence%22%7D&s=10&r=1 [↑](#footnote-ref-3)
3. Margaret Rouse, *Artificial Intelligence (AI)*, Technopedia (Apr. 12, 2024), https://www.techopedia.com/definition/190/artificial-intelligence-ai. [↑](#footnote-ref-4)
4. What is artificial intelligence (AI)?, IBM.com, https://www.ibm.com/topics/artificial-intelligence (last visited May 31, 2024). [↑](#footnote-ref-5)
5. *Federal Communications Commission Technological Advisory Council Meeting,* Dec. 8, 2022, https://www.fcc.gov/sites/default/files/fcc\_tac\_meeting\_slides\_12-08-2022-final.pdf [↑](#footnote-ref-6)
6. Arjun Menon, *Data Poisoning and Its Impact on the AI Ecosystem,* MathCo (Jan. 23, 2023),https://mathco.com/blog/data-poisoning-and-its-impact-on-the-ai-ecosystem [↑](#footnote-ref-7)