



PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov
TTY: 888-835-5322

DA 24-1166
November 20, 2024

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ENCOURAGES COMMUNICATIONS SERVICE PROVIDERS TO IMPLEMENT IMPORTANT NETWORK RELIABILITY BEST PRACTICES

By this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) of the Federal Communications Commission (Commission) reminds communications service providers of the importance of implementing relevant industry-accepted best practices. Earlier this year, the Bureau released its analysis of the facts and circumstances of the February 22, 2024 AT&T Mobility Network Outage,¹ which lasted at least twelve hours and affected users in all 50 states as well as Washington, D.C., Puerto Rico, and the U.S. Virgin Islands.² In the Bureau's assessment, this outage likely could have been prevented or mitigated if the provider had followed best practices recommended by the Commission's Communications Security, Reliability, and Interoperability Council (CSRIC).³ Accordingly, consistent with the recommendations set forth in the Bureau's Report,⁴ we highlight these relevant best practices and encourage providers to integrate them into their policies and procedures where appropriate, to promote network reliability and resiliency in the future. The CSRIC best practices that could have helped prevent or mitigate this outage are listed in the attached Appendix. All of these best practices have been in place for almost a decade or more.⁵

The Bureau highlights two general areas that warrant attention:

- **Change Management:** Recent outage data shows that introducing changes to operational networks through deployment of new platforms, product or software updates, or configuration changes requires careful preparation and planning to reduce the risk of unintended consequences, including network outages. The attached best practices in this area include but are not limited to managing scheduled and unscheduled changes to provider networks; ensuring network integration planning is completed when introducing new network elements; documenting processes for testing, validating, and

¹ See FCC, February 22, 2024 AT&T Mobility Network Outage Report and Findings (2024), <https://www.fcc.gov/document/fcc-issues-report-nationwide-att-mobility-outage> (AT&T Outage Report).

² AT&T Outage Report at 3.

³ CSRIC is a federal advisory committee whose mission is to make recommendations to the Commission to promote the security, reliability, and resiliency of the Nation's communications systems. See FCC, Communications Security, Reliability, and Interoperability Council, (last visited July 29, 2024), <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0> (last visited July 29, 2024).

⁴ AT&T Outage Report at 10 (noting that the Bureau plans to release a Public Notice reminding service providers of the importance of implementing relevant industry-accepted best practices).

⁵ The Commission has made CSRIC best practices and general resources on network reliability available online. See CSRIC Best Practices, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited July 29, 2024); FCC, Network Reliability Resources, <http://www.fcc.gov/network-reliability-resources> (last visited Aug. 28, 2024).

evaluating network changes both before and after implementation, to ensure the results are appropriate and expected; and having a documented back-out plan for scheduled and unscheduled maintenance activities.

- Network Oversight: Failure to ensure there are appropriate checks and balances, such as peer reviews or management reviews and approvals, has contributed to recent outages by enabling errors to propagate from development through implementation. The attached best practices in this area entail documenting policies and enforcing network oversight practices such as installation and maintenance guidelines and communicating the expectation of compliance by all involved parties.

The Bureau reminds communications service providers of the importance of implementing these and other relevant industry accepted best practices to ensure network reliability.

For more information, contact Drew Morin, Deputy Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2336, Drew.Morin@fcc.gov, or Jeanne Stockman, Attorney, Cybersecurity and Communications and Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-7830, Jeanne.Stockman@fcc.gov.

The Public Safety and Homeland Security Bureau issues this Public Notice under delegated authority pursuant to sections 0.191 and 0.392 of the Commission's rules.⁶

⁶ 47 CFR §§ 0.191, 0.392.

APPENDIX

Change Management

- *CSRIC Best Practice 13-10-0418.*¹ Network operators, service providers,² and public safety³ should, where appropriate, have a documented back-out plan as part of a Method of Procedure (MOP) for scheduled and unscheduled maintenance activities.
- *CSRIC Best Practice 13-10-0559.*⁴ Network operators, service providers, and public safety should consider validating upgrades, new procedures and commands in a lab or other test environment that simulates the target network and load prior to the first application in the field.
- *CSRIC Best Practice 13-10-0615.*⁵ Network operators, service providers, and public safety should verify complex configuration changes before committing them and test after the change to ensure the results were appropriate and expected.
- *CSRIC Best Practice 13-9-0574.*⁶ Network operators, service providers, and public safety should actively monitor and manage the 9-1-1 network components using network management controls, where available, to quickly restore 9-1-1 service and provide priority repair during network failure events. When multiple interconnecting providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems.

¹ See CSRIC Best Practice 13-10-0418, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited Aug. 28, 2024).

² “Service providers” includes both covered and originating service providers. “Covered 911 service providers” are defined as “any entity that: [p]rovides 911, E911, or NG911 capabilities such as call routing, automatic location information (ALI), automatic number identification (ANI), or the functional equivalent of those capabilities, directly to a public safety answering point (PSAP) . . . or that [o]perates one or more central offices that directly serve a PSAP.” 47 CFR § 12.4(a)(4)(i)(A)-(B). Originating service providers offer the capability to originate 911 calls, but unlike covered 911 service providers, do not themselves deliver those calls and associated number or location information to the PSAP. See 47 CFR § 12.4(a)(4)(ii)(B). Further, in amendments to 47 CFR § 4.9 that will become effective upon Office of Management and Budget approval as announced in a subsequent public notice, “covered 988 service providers” will be defined as those providers that provide the 988 Lifeline with capabilities such as the ability to receive, process, or forward calls. See *Ensuring the Reliability and Resiliency of the 988 Suicide & Crisis Lifeline; Amendments to Part 4 of the Commission’s Rules Concerning Disruptions to Communications; Implementation of the National Suicide Hotline Improvement Act of 2018*, PS Docket Nos. 23-5, 15-80, and WC Docket No. 18-336, Report and Order, at para. 14, 62 (2023) (*988 Outage Reporting Report and Order*).

³ “Public safety” includes all providers involved in the deployment of 911 networks. See CSRIC, Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and Next Generation 9-1-1 (NG911) Networks, at 5 (Mar. 10, 2021).

⁴ See CSRIC Best Practice 13-10-0559, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited July 29, 2024).

⁵ See CSRIC Best Practice 13-10-0615, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited Aug. 28, 2024).

⁶ See CSRIC Best Practice 13-9-0574, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited Aug. 28, 2024).

- *CSRIC Best Practice 13-8-0590*.⁷ Network operators, service providers, and equipment suppliers should develop MOP for core infrastructure hardware and software growth and change activities and periodically review and update as appropriate.

Network Oversight

- *CSRIC Best Practice 13-9-5196*.⁸ Network operators, service providers, and public safety should ensure that contractors and equipment supplier personnel working in critical network facilities follow the current applicable MOP, which should document the level of oversight necessary.

– FCC –

⁷ See CSRIC Best Practice 13-8-0590, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited Aug. 28, 2024).

⁸ See CSRIC Best Practice 13-9-5196, <https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data> (last visited Aug. 28, 2024).