PUBLIC NOTICE

Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20554

News Media Information 202 / 418-0500
Internet: https://www.fcc.gov
TTY: 1-888-835-5322

DA 20-1406

Released: November 25, 2020

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

PS Docket Nos. 11-60, 20-183

By this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) reminds and encourages communications service providers to follow industry best practices to ensure network reliability, consistent with the recommendations of the Federal Communications Commission's (Commission) Communications Security, Reliability, and Interoperability Council (CSRIC).[1] This reminder also underscores several lessons learned from major communications network outages that occurred this year.[2]

These best practices are summarized as follows:

- *Ensure Sufficient Circuit Diversity*. Network operators, service providers,[3] and public safety entities should periodically audit the physical, logical, and provider diversity in their networks segment(s) to ensure that a single outage will not simultaneously affect different circuits or equivalent data paths.[4]

---

[1] CSRIC is an advisory committee of the Commission. Its 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*, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Nov. 2, 2020). While the Bureau has noted several of these best practices previously, recent outages highlight the need to emphasize these practices again. *See, e.g., Public Safety and Homeland Security Bureau Encourages Communications Service Providers to Implement Important Network Reliability Practices*, DA 19-1039, Public Notice (Oct. 15, 2019), https://docs.fcc.gov/public/attachments/DA-19-1039A1.pdf; *Public Safety and Homeland Security Bureau Encourages Communications Service Providers to Follow Best Practices to Help Ensure Network Reliability*, DA 18-378, Public Notice (Apr. 16, 2018), https://docs.fcc.gov/public/attachments/DA-18-378A1.pdf.

[2] *See* FCC, *June 15, 2020 T-Mobile Network Outage Report*, PS Docket No. 20-183, 16, para. 45 (PSHSB Oct. 2020), https://docs.fcc.gov/public/attachments/DOC-367699A1.pdf (*T-Mobile Report)*.

[3] Here, and in the following CSRIC best practices, "service providers" includes both covered and originating 911 service providers. Covered 911 service providers are defined as any entity that provides 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 operates one or more central offices that directly serve a PSAP. 47 CFR § 9.19(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 § 9.19(a)(4)(ii)(B).

[4] FCC, *CSRIC Best Practices* 12-9-0532, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Nov. 2, 2020); *see also* 47 CFR § 9.19(c)(1) (requiring that covered 911 service providers certify certain activities related to ensuring circuit diversity).

- *Ensure Alternative Routing of 911 Calls*. If primary and secondary routing to 911 call centers, or Public Safety Answering Points (PSAPs), are not available, covered 911 service providers and originating service providers should take steps to ensure that the 911 caller receives assistance, such as routing 911 calls to the administrative lines of destination PSAP(s) and routing any remaining and otherwise undeliverable calls to a common national call center.
- *Validate Network Changes in Test Environment.* Network operators, service providers, and public safety entities 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 actual application in the field.[5]
- *Use Virtual Interfaces*. Service providers should use virtual interfaces for routing protocols and network management to maintain connectivity to network elements in the event of an outage due to the failure of a physical interface (e.g., hardware, fiber link, or cable).[6]
- *Use Network Management Controls*. Network operators, service providers, and public safety entities should actively monitor and manage 911 network components using network management controls, where available, to quickly restore 911 service and provide priority repair during network failure events.[7]
- *Make Spare Equipment Available*. Network operators, service providers, equipment suppliers, and public safety entities should ensure that spare equipment for critical network systems is readily available for replacement purposes,[8] including spare fuses and rectifiers.

Additional information is available at https://www.fcc.gov/network-reliability-resources.

For more information, contact Julia Tu, Engineer, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0731, julia.tu@fcc.gov, or Kathleen Hom, Attorney, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2049, kathleen.hom@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, 47 CFR §§ 0.191, 0.392.

– FCC –

[5] FCC, *CSRIC Best Practices* 12-10-0559, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Nov. 2, 2020); *see* FCC, *CSRIC Best Practices* 12-9-8748, https://opendata.fcc.gov/PublicSafety/CSRIC-Best-Practices/qb45-rw2t/data (stating that network operators, service providers, equipment suppliers, and public safety entities "should test new devices to identify unnecessary services, outdated software versions, missing patches, and misconfigurations, and validate compliance with or deviations from an organization's security policy prior to being placed on a network") (last visited Nov. 2, 2020); FCC, *CSRIC Best Practices* 12-9-8035, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (stating that network operators, service providers, and public safety entities "should include steps to appropriately test all patches and fixes in a test environment prior to distribution into the production environment in their patch/fix policy and process guidelines") (last visited Nov. 2, 2020).

[6] FCC, *CSRIC Best Practices* 12-10-0409, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Nov. 2, 2020).

[7] When multiple interconnecting providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems. FCC, *CSRIC Best Practices* 12-9-0574, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Nov. 2, 2020).

[8] FCC, *CSRIC Best Practices* 12-10-5083, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Nov. 3, 2020).