PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

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

DA 19-1039
October 15, 2019

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

By this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) shares lessons learned from several recent major communications network outages and reminds and encourages communications service providers to review industry best practices to ensure network reliability.[1] These outages could likely have been prevented or mitigated if the providers had followed certain network reliability best practices.

The Bureau encourages communications service providers to implement the following industry best practices, as previously recommended by the Federal Communications Commission's (Commission) Communications Security, Reliability and Interoperability Council (CSRIC):[2]

- *Ensure Sufficient Circuit Diversity*. Network operators, service providers[3] and public safety entities should periodically audit the physical and logical diversity,[4] including provider diversity, in their networks segment(s) to ensure that a single outage won't simultaneously affect different circuits.[5] Covered providers and originating service providers may wish to pursue additional 911-specific actions beyond primary and secondary routing to 911 call centers, or Public Safety Access Points (PSAPs), including a third option to route 911 calls to administrative lines of destination PSAPs and fourth option to route any remaining and otherwise undeliverable calls to a common national call center.
- *Make Spare Equipment Available*. Network operators and service providers should ensure that

[1] *See*, *e.g.*, *December 27, 2018 CenturyLink Network Outage Report* (PSHSB 2019), https://docs.fcc.gov/public/attachments/DOC-359134A1.pdf (*CenturyLink Report*).

[2] 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 VII, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Oct. 4, 2019).

[3] Here, and in the following CSRIC best practices, "service providers" includes both covered and originating service providers. "Covered 911 service providers," or communications service providers that directly serve 911 call centers, 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).

[4] *See also* 47 CFR. §12.4(c) (requiring that covered 911 service providers certify certain activities related to ensuring circuit diversity).

[5] *See* CSRIC Best Practice 11-9-0532, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited September 10, 2019).

spare equipment for critical network systems is readily available for replacement purposes.[6] Network operators and service providers may wish to take steps to ensure that critical spare equipment is maintained in multiple geographic locations, thereby reducing delivery times if the equipment is needed on short notice.

- *Perform Work During Maintenance Windows*. Network operators and service providers should perform work on in-service equipment during maintenance windows (thus during low traffic periods).[7] These entities may wish to implement this practice, especially when making network configuration changes or scheduling procedures that could affect service to a significant number of subscribers.

In addition, the Bureau assesses that the following network operator and service provider practices could prevent or mitigate similar outages in the future:[8]

- Implementing software to detect equipment performance degradation, including by monitoring memory and processor utilization, so that parts likely to fail can be identified and replaced prior to their failure.
- Turning off or disabling system features that are not in use.
- Implementing standard operating procedures for network repair that take effect when normal networking monitoring procedures are inoperable or otherwise unavailable.

The Bureau has a website at https://www.fcc.gov/network-reliability-resources where we share lessons learned from major communications network outages and encourage service providers to review industry best practices to ensure network reliability, including 911 call reliability, at all times.

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 Saswat Misra, Attorney, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0944, Saswat.misra@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 –

[6] *See* CSRIC Best Practice 11-10-5083, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited September 10, 2019).

[7] *See* CSRIC Best Practice 11-10-0693, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited September 10, 2019).

[8] *See*, *e.g.*, CenturyLink Report.