PUBLIC NOTICE

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

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

DA 18-378
April 16, 2018

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ENCOURAGES COMMUNICATIONS SERVICE PROVIDERS TO FOLLOW BEST PRACTICES TO HELP ENSURE NETWORK RELIABILITY

By this Public Notice, the Public Safety and Homeland Security Bureau (Bureau) disseminates lessons learned from major network outages, and it reminds and encourages communications service providers to review industry best practices to ensure network reliability. The Bureau also recommends that communications service providers visit the Bureau's new network reliability page on its website to help ensure that network providers, public safety entities, and the general public can readily find the Bureau's work in promoting industry best practices. The website can be found at http://www.fcc.gov/network-reliability-resources.

Based on its recent analysis of several major network outages that affected subscribers, including those calling 911 for emergency assistance, Bureau staff determined that the outages could likely have been prevented or mitigated if the provider had followed certain network reliability best practices. Therefore, the Bureau encourages communications service providers to implement the following industry best practices, as previously recommended by the Commission's Communications Security, Reliability and Interoperability Council:[1]

1. *Minimize Impact of Maintenance Windows*. Network operators and service providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (*e.g.*, maintenance, high-risk procedures, growth activities) to minimize the impact on end-user services.[2]
2. *Monitor 911 Network Components*. Network operators, service providers, and public safety entities should actively monitor and manage the 911 network components using network management controls, where available, to quickly restore 911 service and provide priority repair during network failure events. When multiple interconnecting

[1] CSRIC is an advisory committee of the Federal Communications Commission, the mission of which is to make recommendations to the Commission to promote the security, reliability and resiliency of the Nation's communications systems. FCC, Communications Security, Reliability, and Interoperability Council (CSRIC), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

[2] Communications Security, Reliability and Interoperability Council, Best Practice 9-9-0595 (2011), https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems.[3]

3. *Ensure Real-World Testing Conditions*. Service providers and network operators 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.[4]

In addition, the Bureau assesses that the following practices could prevent or mitigate similar outages in the future:

1. *Registration Traffic*. Include registration traffic in the highest priority category of network traffic. Attach critical alarms to failures in the registration process.
2. *Data Packet Monitoring*. Monitor traffic to detect when data packets do not progress across a network element.
3. *Redundancy Failover.* Fail over to redundant equipment when the number of error messages within a pre-determined period of time exceeds a certain threshold, rather than continuing to try to use the equipment that is generating the error messages.
4. *Redundancy During Maintenance*. When performing maintenance activity on multiple pieces of equipment that have the same function for redundancy, perform maintenance on only one piece of equipment at a time. Once successful maintenance has been verified, maintenance activity can begin on the next piece of equipment.

For more information, contact John Healy, Associate Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2448, john.healy@fcc.gov, or Robert M. Finley, Attorney, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-7835, robert.finley@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-

[3] Communications Security, Reliability and Interoperability Council, Best Practice 9-9-0574 (2011), https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

[4] Communications Security, Reliability and Interoperability Council, Best Practice 9-7-0559 (2011), https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.