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 17-672
Released: July 12, 2017

FCC'S PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REMINDS COMMUNICATIONS SERVICE PROVIDERS OF IMPORTANCE OF IMPLEMENTING NETWORK RELIABILITY BEST PRACTICES

PS Docket No. 17-68

The Federal Communications Commission's (Commission's) Public Safety and Homeland Security Bureau (Bureau) encourages communications service providers to implement appropriate measures to prevent major service disruptions.

Based on submissions to the Commission's Network Outage Reporting System (NORS) and publicly available data, the Bureau has observed a number of major service outages caused by minor changes in network management systems.[1] These so-called "sunny day" outages do not result from a natural weather-related disaster or other unforeseeable catastrophe, and can result in "silent failures," which are outages that occur without providing explicit notification or alarm to the service provider.[2] In 2014, the Bureau first highlighted the occurrence of major "sunny day" outages affecting users in multiple states.[3] These major outages continue to occur, some affecting users nationwide.[4] Outages that impact 911 service are of particular concern, given the importance of ensuring continuity of 911 service.

After an analysis of the facts and circumstances, Bureau staff have determined that service providers likely could have prevented most of these outages if they had implemented certain industry best practices. In particular, seven best practices recommended by the Commission's Communications Security Reliability and Interoperability Council (CSRIC) II,[5] a former federal advisory committee, could help prevent sunny day outages and silent failures:

[1] NORS is the web-based filing system through which communications providers submit reports of service disruptions to the FCC. *See* 47 CFR Part 4. NORS information is presumed to be confidential and protected from routine public disclosure. Commission staff regularly aggregates and analyzes data to identify trends in outages. When releasing aggregate information to the public, staff removes provider-identifying information to preserve providers' confidentiality.

[2] *See*, *e.g.*, Bob Brown, Level 3 Acknowledges Network Outage, Network World (Oct. 4, 2016, 9:07 AM), http://www.networkworld.com/article/3127062/lan-wan/level-3-acknowledges-network-outage.html.

[3] *See* PSHSB, April 2014 Multistate 911 Outage: Cause and Impact, PS Docket No. 14-72, at 1 (2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-330012A1.pdf.

[4] *See*, *e.g.*, PSHSB, March 8th, 2017 AT&T VoLTE 911 Outage Report and Recommendations, PS Docket No. 17-68, at 3 (2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0518/DOC-344941A1.pdf (reporting the Bureau's findings on a nationwide Voice over LTE (VoLTE) 911 outage that prevented approximately 12,600 911 callers from reaching 911 directly).

[5] CSRIC is a Federal Advisory Committee established pursuant to the Federal Advisory Committee Act to advise the Commission regarding network reliability and interoperability. *See* 5 U.S.C. App. 2; *see also* FCC Open Data,

(continued….)

1. **Awareness Training**: "Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements."[6]
2. **Required Experience and Training**: "Network Operators, Service Providers, and Equipment Suppliers should establish a minimum set of work experience and training courses which must be completed before personnel may be assigned to perform maintenance activities on production network elements, especially when new technology is introduced in the network."[7]
3. **Access Privileges**: "Service Providers, Network Operators, and Equipment Suppliers should have policies on changes to and removal of access privileges upon staff member status changes."[8]
4. **Network Change Verification**: "Network Operators should establish policies and processes for adding and configuring network elements that include approval for additions and changes to configuration tables (*e.g.*, screening tables, call tables, trusted hosts, and calling card tables. Verification rules should minimize the possibility of receiving inappropriate messages."[9]
5. **Network Reconfiguration 911 Assessment**: "Service Providers and Network Operators when reconfiguring their network (*e.g.*, changes to Virtual Private Cloud (VPC), Mobile Position Center (MPC), Gateway Mobile Location Center (GMLC), or Emergency Services Gateway (ESGW)) should assess the impact on the routing of 911 calls."[10]
6. **Diversity Audits**: "Network Operators and Public Safety should periodically audit the physical and logical diversity called for by network design of their network segment(s) and take appropriate measures as needed."[11]
7. **Network Monitoring**: "Network Operators, Service Providers, and Public Safety should monitor their network to enable quick response to network issues."[12]

The Bureau encourages service providers to review and consider voluntarily implementing these network reliability best practices as appropriate.[13]

(Continued from previous page)
CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 22, 2017) (providing an indexed database of network reliability best practices developed by CSRIC II);

[6] CSRIC II Best Practice 9-7-0588, https://www.fcc.gov/nors/outage/bestpractice/DetailedBestPractice.cfm?number=9-7-0588 (last visited Jun. 9, 2017).

[7] *See* CSRIC II Best Practice 9-7-0589, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 9, 2017).

[8] *See* CSRIC II Best Practice 9-8-8098, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 9, 2017).

[9] *See* CSRIC II Best Practice 9-9-8729, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 9, 2017).

[10] *See* CSRIC II Best Practice 9-9-0902, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 9, 2017).

[11] *See* CSRIC II Best Practice 9-9-0532, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 9, 2017).

[12] *See* CSRIC II Best Practice 9-9-0401, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Jun. 9, 2017).

In addition to considering CSRIC-recommended best practices, the Bureau also recommends that service providers consider implementing the following lessons learned derived from the Bureau's fact-based analysis of several recent outages.[14] The Bureau finds that taking these steps could help to prevent future outages or mitigate the impact of outages that do occur.

- **Access Control**: Limit direct access to operations support systems that control a large number of switches, soft switches, or routers.
- **Validation and Authentication**: Implement validation and authentication procedures for any changes that affect call routing.
- **Software-based Alarming**: Work with vendors to implement software that warns technicians when a change is being made that could potentially affect a large number of calls or customers.
- **Enhanced Outage Detection**: Implement traffic measurements or other mechanisms in major network elements to enable the detection of failures where calls are lost but associated equipment continues to operate.
- **Automatic Re-routing**: Examine whether automatic re-routing of calls would be an effective remediation strategy in the event of outages.

For further 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 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 –

(Continued from previous page)

[13] *See also* ATIS, Network Reliability Steering Committee (NSRC) Bulletin No. 2017-002, "Silent Alarm Failures" Investigation (2017), https://www.atis.org/docstore/product.aspx?id=28312 (providing industry recommendations to reduce the frequency of silent failures).

[14] *See* PSHSB, March 8th, 2017 AT&T VoLTE 911 Outage Report and Recommendations, PS Docket No. 17-68, at 3 (2017), http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0518/DOC-344941A1.pdf. This report set forth the Bureau's findings in connection with its investigation of the March 8th outage and noted that the outage offered an illuminating case study of actions that stakeholders can take to promote network reliability and continued access to 911 service. The report also identified the need for further outreach and for close working coordination between public safety stakeholders. To this end, the Bureau will be holding a workshop to discuss best practices and develop recommendations for improving situational awareness during 911 outages. This workshop will be announced by a subsequent Public Notice.