PUBLIC NOTICE

DA 17-1029
Released: October 19, 2017

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ENCOURAGES VOLUNTARY ADOPTION OF NETWORK RELIABILITY BEST PRACTICES BY SMALL AND RURAL SERVICES PROVIDERS

The Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (Bureau) encourages small and rural communications service providers to review and consider implementing, where appropriate, best practices recommended by the Communications Security, Reliability, and Interoperability Council (CSRIC), a federal advisory committee to the FCC,[1] to improve network reliability.

Network reliability and resiliency is essential to ensure that all consumers, public safety entities, and small businesses have access to reliable and secure communications, especially during disasters and emergencies. Since its inception, CSRIC has identified over a thousand best practices to improve the reliability of communications networks.[2]

As part of the Commission's ongoing efforts to support small and rural providers, the Bureau has reviewed the CSRIC best practices and outage data from the Commission's Network Outage Reporting System (NORS)[3] to identify trends and common failures among outages experienced by small and rural service providers.[4] This process identified 23 of the most recurring best practices (see Appendix I) reported in NORS outage reports during the last five years as filed by small and rural communications providers. Providers cited these best practices in their final reports as ones which may have helped to prevent such outages had they been implemented. The Bureau encourages small and rural communications services providers to review and consider these 23 best practices along with other CSRIC best practices as appropriate for their networks.

These 23 best practices do not reflect an exhaustive list of applicable best practices as small and rural communications providers may implement other best practices not reflected in this list. We welcome any feedback from small and rural providers about these best practices. For further information, contact Jennifer Holtz, Deputy Division Chief, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-2336, Jennifer.Holtz@fcc.gov or Steven

---

[1] FCC, Communications Security, Reliability, and Interoperability Council, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0 (last visited Sept. 29, 2017).

[2] FCC Open Data, CSRIC Best Practices, https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data (last visited Sept. 29, 2017).

[3] NORS is a web-based filing system through which communications providers are required to electronically report information about significant disruptions or outages to their communications systems affecting a certain number of customers over a specified amount of time set forth in Part 4 of the FCC's rules (47 C.F.R. pt. 4).

[4] The Bureau reviewed all the CSRIC best practices identified by all services providers in their outage reports from last five years except those filed by nationwide communications providers.

McKinnon, Electronics Engineer, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-0390, Steven.McKinnon@fcc.gov

Appendix I:
Best Practices Applicable to Small and Rural Providers (2013-2017)

Best Practice Number[5]	Description	Network Type(s)[6]
9-9-5196	Network Operators, Public Safety and Service Providers should ensure that contractors and Equipment Supplier personnel working in critical network facilities follow the current applicable MOP (Method of Procedures), which should document the level of oversight necessary.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-7-0634	Network Operators, Service Providers and Property Managers together with the Power Company and other tenants in the location, should verify that aerial power lines are not in conflict with hazards that could produce a loss of service during high winds or icy conditions.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-7-0492	Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-7-0495	Network Operators and Property Managers should consider pre-arranging contact information and access to restoral information with local power companies.	Wireless
9-9-0568	Network Operators, Service Providers and Public Safety should establish a routing plan so that in the case of lost connectivity or disaster impact affecting a Public Safety Answering Point (PSAP), 9-1-1 calls are routed to an alternate PSAP answering point.	Cable; Internet/Data; Wireline
9-7-0493	Network Operators and Property Managers should consider placing fixed power generators at cell sites, where feasible.	Wireless
9-9-0476	Network Operators, Public Safety, and Property Managers should consider conducting physical site audits after a major event (e.g., weather, earthquake, auto wreck) to ensure the physical integrity and orientation of hardware has not been compromised.	Wireless
9-9-0546	Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).	Cable; Internet/Data; Satellite; Wireless; Wireline

---

[5] See Best Practices Numbering Format at http://www.atis.org/bestpractices/Tutorial.aspx#4 (last visited Sept. 29, 2017).
[6] Relevant types of communications networks applicable to each best practice.

Best Practice Number[5]	Description	Network Type(s)[6]
9-9-0566	Network Operators, Service Providers and Public Safety should consider placing and maintaining 9-1-1 TDM or IP based networks over diverse interoffice transport facilities (e.g., geographically diverse facility routes, automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof).	Cable; Internet/Data; Wireless; Wireline
9-9-0612	Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-7-5058	Back-up Power: Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-1028	Network Operators, Service Providers, Public Safety and Property Managers should engage in preventative maintenance programs for network site support systems including emergency power generators, UPS, DC plant (including batteries), HVAC units, and fire suppression systems.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-5113	Network Operators, Service Providers, Public Safety and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF).	Cable; Internet/Data; Satellite; Wireless; Wireline
9-7-0650	Network Operators, Service Providers and Property Managers should place strong emphasis on human activities related to the operation of power systems (e.g., maintenance procedures, alarm system operation, response procedures, and training) for operations personnel.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-0401	Network Operators, Service Providers, and Public Safety should monitor their network to enable quick response to network issues.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-0574	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.	Cable; Internet/Data; Wireline
9-9-0577	Network Operators, Service Providers and Public Safety responsible for Public Safety Answering Point (PSAP) operations should jointly and periodically test and verify that critical components (e.g., automatic re-routes, PSAP Make Busy keys) included in contingency plans work as designed.	Cable; Internet/Data; Wireless; Wireline

Best Practice Number[5]	Description	Network Type(s)[6]
9-9-0758	Network Operators, Service Providers and Public Safety should, upon restoration of service in the case of an outage where 9-1-1 call completion is affected, make/request multiple test calls to the affected PSAP(s) to ensure proper completion.	Cable; Internet/Data; Wireless; Wireline
9-9-0786	Network Operators, Service Providers, and Public Safety should consider allowing Equipment Suppliers or third party Service Providers remote secured access to vital hardware components.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-1022	Network Operators, Service Providers, Public Safety, and Equipment Suppliers should consider the development of a vital records program to protect vital records that may be critical to restoration efforts.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-1033	Network Operators should develop a strategy for deployment of emergency mobile assets such as Cell on Wheels (COWs), cellular repeaters, Switch on Wheels (SOWs), transportable satellite terminals, microwave equipment, power generators, HVAC units, etc. for emergency use or service augmentation for planned events (e.g., National Special Security Event (NSSE)).	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-5204	Service Providers, Network Operators, Public Safety and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.	Cable; Internet/Data; Satellite; Wireless; Wireline
9-9-5207	Network Operators, Service Providers, Public Safety and Property Managers should take appropriate precautions to ensure that fuel supplies and alternate sources of power are available for critical installations in the event of major disruptions in a geographic area (e.g., hurricane, earthquake, pipeline disruption). Consider contingency contracts in advance with clear terms and conditions (e.g., Delivery time commitments, T&Cs).	Cable; Internet/Data; Satellite; Wireless; Wireline