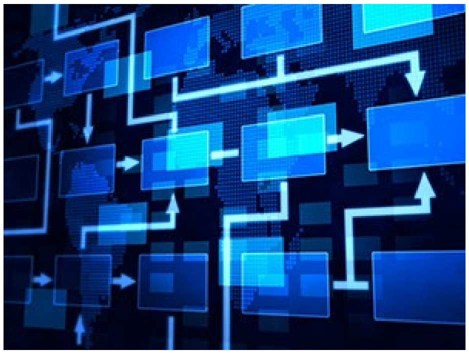
FCC (Again) Takes to Bully Pulpit to Urge Network Reliability "Best Practices" to Combat Service Outages

July 14, 2017



On July 12, 2017, the Public Safety and Homeland Security Bureau ("Bureau") of the Federal Communications Commission ("FCC") issued a Public Notice encouraging communications service providers to implement certain "best practices" to avoid major service disruptions. The Bureau's recommendations come on the heels of recent major service outages caused by minor changes to service providers' network management systems that knocked out 911 service. These service disruptions are known as "sunny day" outages because they are not caused by weather-related issues or other disasters, but rather internal network management failures due to faulty software or botched upgrades. The Bureau's recommendations serve as a warning to service providers, but do not (at this time at least) have an enforceable effect on providers.

Under the FCC's rules, communications service providers, including wireline, wireless, cable, satellite VoIP, and others are required to electronically report through the FCC's Network Outage Reporting System ("NORS") significant disruptions to their communications systems that meet specified thresholds based on the area or amount of consumers impacted. The Bureau recommendations show that the FCC analyzes this data, particularly in light of the recent sunny day outages that have garnered publicity.

The Bureau outlined seven best practices to help prevent such outages:

1. Awareness Training: Service providers should make all personnel involved in the operation, maintenance, security, and support of their networks aware of outage risks and the impact of network failures;

2. Required Experience and Training: Service providers should establish a minimum set of work experience and training courses that must be completed before personnel may be assigned to perform maintenance on their networks, especially when the maintenance involves upgrades to new technologies;

3. Access Privileges: Service providers should adopt policies regarding who has access to their networks and procedures for changing and removing access privileges;

4. Network Change Verification: Service providers should adopt procedures for verifying any changes to the operations of their networks before implementation;

5. Network Reconfiguration 911 Assessment: Service providers should assess the impact of any network reconfiguration on 911 call routing before carrying out any changes;

6. Diversity Audits: Service providers should periodically audit the physical and logical “diversity” (*e.*, redundancy) of their networks and take action to ensure continued service in response to uncovered risks; and

7. Network Monitoring: Service providers should actively monitor their networks to enable quick responses to outages and other issues.

The Bureau further recommended that service providers consider implementing five additional practices that likely would have prevented the recent major 911 service outages:

1. Access Control: Service providers should limit personnel access to network management support systems that that control a large number of switches, soft switches, or routers;

2. Validation and Authentication: Service providers should implement validation and authentication procedures for any changes that affect call routing, not just changes impacting 911 calls;

3. Software-based Alarming: Service providers should implement software that warns them when a network change is being made that could potentially affect a large number of calls;

4. Enhanced Outage Detection: Service providers should implement traffic measurements or other mechanisms to enable them to detect “silent failures,” where calls are lost but associated equipment continues to operate; and

5. Automatic Re-routing: Service providers should consider implementing automatic re-routing of calls in the event of outages.

The best practices and suggestions included in the Public Notice are voluntary, but the Bureau noted that it regularly reviews reports filed through NORS to identify outage trends and identify deficiencies in service provider practices. The Public Notice’s is forward-focused, analyzing past outages in order to improve outage-prevention measures. The Public Notice is consistent with the FCC’s prior emphasis on industry adoption of voluntary best practices, instead of using the “big stick” of enforcement penalties against service providers in response to outages.