United States Government Accountability Office

Report to the Ranking Member, Committee on Energy and Commerce, House of Representatives

December 2017

TELECOMMUNICATIONS

FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency

Accessible Version

GAO
Highlights

Highlights of GAO-18-198, a report to the Ranking Member, Committee on Energy and Commerce, House of Representatives

December 2017

TELECOMMUNICATIONS

FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency

Why GAO Did This Study

Americans increasingly rely on mobile wireless communications for safety-related communications like calling 911 and receiving weather alerts. Mobile wireless networks face risks from physical incidents including extreme weather events and intentional and accidental damage. For example, in 2017 several major hurricanes damaged wireless network infrastructure, leaving many U.S. citizens without reliable access to wireless communications.

GAO was asked to review federal efforts to improve the resiliency of wireless networks following natural disasters and other physical incidents. This report examines: (1) trends in mobile wireless outages reported to FCC since 2009 and (2) actions federal agencies and industry have taken since 2013 (after Hurricane Sandy) to improve wireless network resiliency, among other objectives. GAO analyzed wireless outage data from 2009 to 2016 (4 years before and after Hurricane Sandy); reviewed FCC, DHS, and industry documents; and interviewed stakeholders who represented a variety of perspectives, such as industry, public safety, and consumer groups. GAO assessed FCC's efforts to monitor an industry initiative to improve wireless network resiliency against federal internal control standards.

What GAO Recommends

FCC should work with industry to develop specific performance measures for the Wireless Network Resiliency Cooperative Framework, monitor the framework's outcomes, and promote awareness of it. FCC agreed with the recommendations.

View GAO-18-198. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

What GAO Found

The number of wireless outages attributed to a physical incident—a natural disaster, accident, or other manmade event, such as vandalism—increased from 2009 to 2016, as reported to the Federal Communications Commission (FCC). During this time, the number of outages substantially increased from 189 to 1,079 outages, with most of the increase occurring from 2009 to 2011. FCC officials said this increase was due in part to growth in wireless customers and wireless infrastructure. Almost all outages attributed to a physical incident were due to an accident, such as damage to a cable due to a digging error (74 percent) or a natural disaster (25 percent). However, outages due to a natural disaster had a longer median duration (ranging from 19 to 36 hours), which was more than twice as long as outages caused by an accident. Power failures and failures in other providers' networks also play a role in wireless outages attributed to physical incidents. For instance, carriers reported that 87 percent of wireless outages attributed to a physical incident were due to a failure in another provider's network on which they rely.

Since 2013, federal agencies and industry have taken actions to improve the resiliency of wireless networks. For example, the Department of Homeland Security (DHS) and FCC charter federal advisory committees that have examined resiliency issues and potential solutions, such as sharing infrastructure during emergencies. FCC also proposed a rule that would disclose how individual wireless carriers' networks performed during emergency events. In response, an industry coalition announced an initiative—the Wireless Network Resiliency Cooperative Framework—whereby carriers agreed to allow roaming on each other's networks and aggregated statistics to be published on how networks performed during emergency events. This initiative prompted FCC to not adopt its proposed rule. FCC said it would engage with industry about the framework's implementation and use, but FCC has limited formal plans to oversee or spread knowledge of the framework:

- FCC developed a plan to track the completion of initial implementation tasks outlined in the framework, but this plan does not include steps to track or evaluate any outputs or outcomes from the framework.
- FCC and industry documents describe broad goals for the framework, such as advancing information sharing during and after emergency events, but neither FCC nor industry has set any specific measures to help determine whether the framework achieves these broad goals.
- Although some public safety officials and other stakeholders GAO contacted were not aware of the framework, FCC did not have plans to actively communicate information about the framework to these audiences.

More robust measures and a better plan to monitor the framework would help FCC collect information on the framework and evaluate its effectiveness. Such steps could help FCC address any challenges or decide whether further action is needed. Also, by promoting awareness about the framework, FCC would help public safety officials and other industry participants to be well positioned to use the framework to help them prepare for or respond to emergency events.

Contents

Tables

Figures

Abbreviations

CSRIC	Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
DIRS	Disaster Information Reporting System
ESF-2	Emergency Support Function #2 – Communications
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
NCC	National Coordinating Center for Communications
NIST	National Institute of Standards and Technology
NORS	Network Outage Reporting System
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long-Term Evolution

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 12, 2017

The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

Dear Mr. Pallone:

Americans are increasingly reliant on mobile wireless communications in their day-to-day lives to make phone calls and share information through the Internet, including for safety-related communications, such as making 911 calls and receiving weather alerts. The nation's mobile wireless networks face risks from a variety of physical incidents including extreme weather events and accidents, such as backhoe cuts to cables connecting cell towers to the broader network. In recent years, major storms have caused outages in mobile wireless networks, severely impairing safety communications when they were most needed. For example, several major hurricanes made landfall in the United States in August and September 2017, damaging wireless network infrastructure and causing power outages that led to localized wireless outages. This included Hurricane Irma—which caused extreme damage in the U.S. Virgin Islands, Puerto Rico, and Florida, among other states—and Hurricane Maria that severely affected infrastructure including wireless networks in Puerto Rico and the U.S. Virgin Islands. As a result of Hurricane Maria, a majority of all cell sites were knocked out of service for months, leaving residents without reliable and continuous access to voice and data communications.[1]

As citizens and public safety officials—such as police officers, firefighters, and emergency medical-services personnel—are increasingly dependent on wireless communications, federal agencies and the communications sector have stressed the importance of resilient mobile wireless communications during times of emergency. As of 2016, over 65 percent of households in the United States relied solely or mostly on wireless

[1] A cell site is defined as the entire set of equipment needed to receive and transmit radio signals for cellular voice and data transmission.

phones to make and receive phone calls.[2] Further, according to the Federal Communications Commission (FCC), about 70 percent of calls to 911 are made from wireless devices. The private sector owns and operates the nation's wireless networks as well as other communication networks and is primarily responsible for managing and protecting these assets. However, the federal government plays a role in promoting wireless network resiliency—that is, the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.[3] FCC is the federal regulatory agency for communications and its mission includes promoting the safety of life and property through the use of radio communications. The Department of Homeland Security (DHS) is responsible for coordinating the federal effort to promote the security and resilience of the nation's critical infrastructure, which includes the communications sector, and also serves as the lead agency for coordinating and prioritizing security and resiliency activities in the communications sector. Further, communications networks are especially important due to the enabling functions they provide across all critical infrastructure sectors; the loss of communications facilities could have cascading effects on other critical infrastructures due to interdependencies among sectors.[4]

You asked us to review efforts that have been taken since Hurricane Sandy in late 2012 to improve the resiliency of mobile wireless networks as well as options that federal agencies could take to enhance wireless resiliency following natural disasters and other physical incidents. This report examines: (1) trends in mobile wireless outages attributed to physical incidents since 2009 as reported to FCC, (2) the actions federal agencies and industry have taken since 2013 to improve wireless network resiliency, and (3) options that federal agencies could take to improve network resiliency and their advantages and disadvantages. This report focuses on the physical risks facing wireless networks; in other words, the

[2] Centers for Disease Control and Prevention, U.S. Department of Health and Human Services, *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey, July–December 2016* (Atlanta, GA: May 2017).

[3] The White House, *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013).

[4] According to a presidential directive, there are 16 critical infrastructure sectors that are so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health, or safety. The directive also identified lead federal agencies to coordinate and prioritize security and resiliency activities in each sector. *Presidential Policy Directive/PPD-21*.

potential for an unwanted effect from an incident on a network's infrastructure such as towers, antennas, and switches. Therefore, we did not examine cyber risks facing wireless networks.[5]

To address these objectives, we analyzed data submitted by wireless carriers to FCC's Network Outage Reporting System (NORS) on wireless outages that occurred from 2009 through 2016 (that is, to cover 4 years of data before and after Hurricane Sandy).[6] In particular, we determined the total number and causes of wireless outages that were reported as having occurred during that time period and identified the share of all wireless outages attributed to a physical incident. We analyzed other characteristics of wireless outages such as location, duration, and whether the failure occurred in another company's network. We took several steps to assess the reliability of NORS data, such as reviewing FCC documentation and interviewing agency officials responsible for collecting and analyzing NORS data, and found the data were sufficiently reliable for the purposes of describing trends in wireless outages.

We also reviewed reports and documents from FCC, DHS, and the National Institute of Standards and Technology (NIST); federal advisory committees and partnership councils that cover wireless network resiliency; and industry. We interviewed officials from FCC, NIST, and several DHS component agencies responsible for protecting and securing the communications infrastructure, as well as representatives from 24 stakeholders, selected to ensure we covered different perspectives. Stakeholders included five wireless carriers and two owners of other wireless network infrastructure, seven industry associations, three consumer groups, five state and local government officials, one partnership council, and one representative from academia. We selected wireless carriers and owners of other wireless network infrastructure to ensure variety in company size and industry role. We selected state agencies to include states directly affected by two events in 2016—flooding in Louisiana and Hurricane Matthew—for which industry had

[5] We have previously examined cyber risks facing communications networks and critical infrastructure sectors. See GAO, *Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts*, GAO-13-275 (Washington, D.C.: Apr. 3, 2013), and GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, GAO-16-79 (Washington, D.C.: Nov. 19, 2015).

[6] Our analysis of NORS data does not include any outages from 2017 (such as outages caused by hurricanes Harvey, Irma, or Maria).

implemented elements of the framework at the time we began our review. However, the views presented in our report are not generalizable to those of all stakeholders.

We assessed FCC's efforts to monitor an industry initiative to improve wireless network resiliency against federal standards for internal control and FCC's current strategic plan.[7] We identified options for improving wireless network resiliency by examining federal agency reports, literature, and other sources. We obtained stakeholder views on the advantages, disadvantages, and feasibility of the identified options by using open-ended questions to solicit input. Appendix I describes our scope and methodology in greater detail.

We conducted this performance audit from January 2017 to December 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

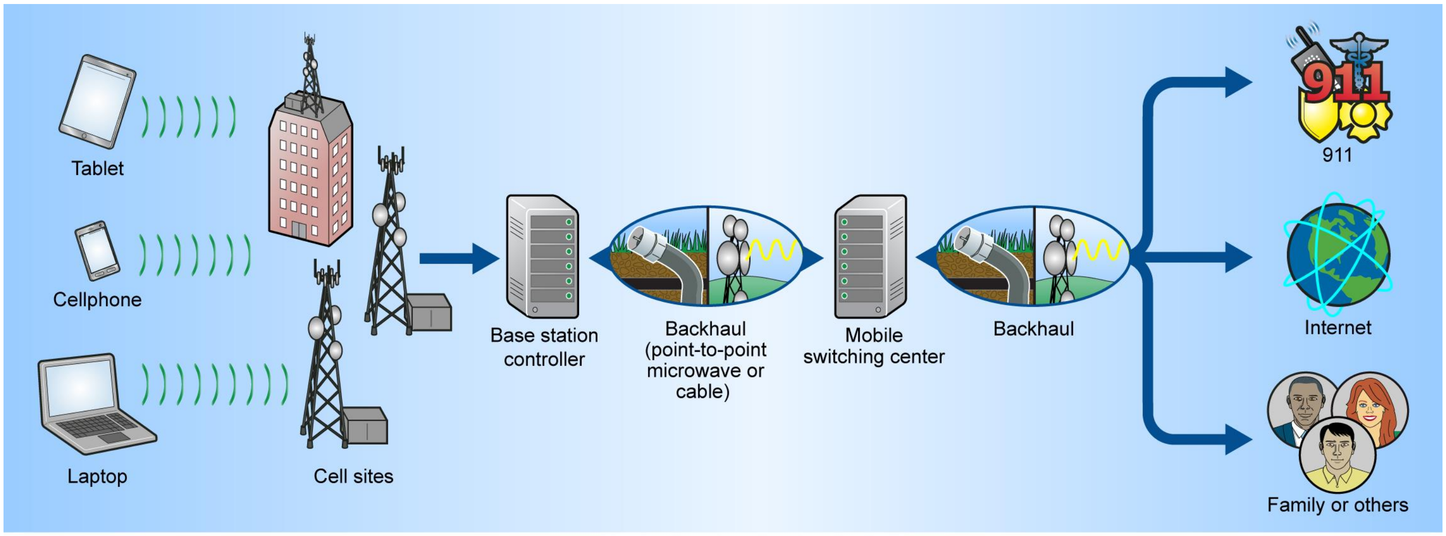
Mobile devices use wireless networks to enable voice and data communications. Mobile wireless networks comprise several components and provide coverage based on dividing a large geographic area into smaller areas of coverage known as "cells." Each cell contains a cell site—a base station equipped with an antenna—to receive and transmit radio signals to mobile devices within its coverage area. (See fig. 1.) The cell sites are often located on a tower, rooftop, or other structure to provide coverage to a wide area.[8] For a mobile device to transmit and receive signals, it must be within range of a cell site antenna. In many

[7] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014) and FCC, *Strategic Plan, 2015–2018* (Washington, D.C.).

[8] In some areas, small cell infrastructure is used to add capacity or expand coverage, including the use of distributed antenna systems and small cell technologies. A distributed antenna system is a network of antennas that is generally connected by fiber optic cables to the broader wireless network. Small cells refer to low-powered access nodes deployed at a particular location. Small cells typically have a range from about 10 to several hundred yards. Large cell sites, by contrast, can have a range of about 20 miles.

areas, a mobile device is able to transmit and receive signals from multiple cell sites. Each cell site is linked to a base station controller that manages communications between the cell site and the mobile switching center (e.g., routes and hands over calls). The mobile switching center then directs voice and data traffic to landline phones, other cell phones via a carrier's network, or the Internet. Backhaul facilities provide transport for this voice and data traffic, and backhaul can be provided over fiber optic or copper cables or wirelessly via microwave facilities.

Figure 1: Example of Mobile Wireless Network Components



Source: GAO. | GAO-18-198

According to FCC, there are four "nationwide" mobile wireless carriers—AT&T, Verizon, T-Mobile, and Sprint—with networks that cover most of the United States. The industry also includes dozens of other carriers, many of which provide service in a specific, sometimes rural, geographic area.[9] According to an FCC report on the wireless industry, most consumers in the United States have the ability to choose among multiple carriers with wireless network coverage in their area, and wireless carriers typically compete on price, network quality, and the availability of mobile devices with innovative features. Federal law states that FCC

[9] The wireless industry also includes resellers and mobile virtual-network operators, which purchase mobile wireless service wholesale from facilities-based carriers and resell the service to consumers. Since these operators do not own or operate their own facilities and our focus is on physical risks to wireless networks, these operators are not a focus of this report.

must take into account whether its actions will encourage competition in mobile wireless networks.[10] Some wireless carriers own a portion or all of the structures that host cell sites, but wireless carriers mostly lease space from independent companies that own or operate a majority of the towers and other structures that host cell sites.

Mobile wireless networks face several kinds of risks that could affect the network's physical components, resulting in disrupted service or an outage. Government reports generally identify three types of physical risks facing wireless networks:

- Natural disasters, such as hurricanes, tornados, wildfires, and earthquakes.
- Manmade events, such as terrorist attacks and damage associated with theft or another malicious act.
- Accidents, such as cable damage due to digging or locating errors and damage associated with a vehicle accident.

The potential effects related to these physical risks include damage to wireless network components that requires wireless carriers and other providers to make repairs or replace equipment to restore service. For example, flooding, which can occur with a hurricane or heavy rain, could damage the cable or other equipment submerged in water. Wildfires can damage network components like antennas and backhaul facilities (including fiber optic and copper lines and microwave towers) as well as equipment in buildings if the buildings are damaged or destroyed.

In addition to physical risks, wireless networks face risks stemming from their dependence on other sectors and providers. One key dependency identified by several government and industry reports is the reliance on commercially provided electricity, referred to in this report as commercial power.[11] Several components—including the mobile switching center, antennas at cell sites, and consumer devices—may rely on commercial power. Therefore, loss of electric power may result in a loss of wireless communications. Another key dependency for wireless networks is backhaul used to get data from an end user to a major network. Wireless

[10] 47 U.S.C. § 332.

[11] We previously examined federal efforts to improve the resiliency of the electricity grid. See GAO, *Electricity: Federal Efforts to Enhance Grid Resilience,* GAO-17-153 (Washington, D.C.: Jan. 25, 2017).

carriers can provide backhaul but typically obtain it from another communications provider, such as a local telephone company or cable company. An outage in the backhaul network can cause an outage that affects one or more cell sites or a portion of the wireless network. FCC has reported that the loss of backhaul service is a major cause of a cell site's unavailability, which can lead to wireless outages. Also important is having clear roads and highways, as wireless carriers' personnel or contractors need to be able to access cell sites to repair or replace equipment, or deliver fuel for generators that are sometimes located at cell sites.

Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, according to *Presidential Policy Directive 21*.[12] Owners and operators of wireless networks can take a variety of actions to manage different risks, including various physical risks, according to the *Communications Sector-Specific Plan*.[13] These actions can be designed to achieve different aims, including to

- prepare for incidents, like creating and exercising disaster recovery plans;
- reduce a specific vulnerability, like elevating or moving a mobile switching center in a flood-prone area to a higher location;
- mitigate the consequences of an incident, like installing backup power—using batteries with a limited supply of power or generators that run on diesel or other fuel sources—to support continued wireless service during a commercial power outage; or
- enable efficient response and restoration following an incident, such as deploying portable cell sites on trucks and other equipment after an incident to provide wireless communications when the network experiences an outage or a significant disruption.

FCC, pursuant to the Communications Act of 1934, as amended, is charged with regulating interstate and international communications throughout the United States, which means that FCC regulates wireless

[12] *Presidential Policy Directive/PPD-21*.

[13] DHS, *Communications Sector-Specific Plan, An Annex to the NIPP 2013* (Washington, D.C.: 2015). This plan sets goals to guide the sector's voluntary efforts to improve security and resilience over the following 4 years.

networks and carriers, among other responsibilities.[14] It develops and administers policies and rules to advance the security and reliability of the nation's communications infrastructure; this responsibility includes, among other topics, network resiliency, public safety communications, and communications infrastructure protection.[15] FCC administers two web-based outage-reporting systems to help it oversee network reliability and resiliency:

- NORS: Carriers are required to report details about service disruptions or outages (e.g., cause, location, and duration) to their communications systems that meet specified thresholds set forth in regulation.[16] FCC uses NORS data to monitor trends in communications outages and to try to identify and address any shortcomings or issues going forward.
- Disaster Information Reporting System (DIRS): Carriers can voluntarily report on the status of communications infrastructure during an emergency event in DIRS. For example, wireless carriers report daily on the number of cell sites, by county, that are out of service by reason (e.g., power outage, physical damage). FCC activates DIRS in response to an event and then uses these data to track network restoration during and after an emergency event.

DHS also plays a role in wireless network resiliency as the lead agency for coordinating and prioritizing security and resilience activities for the communications sector. *Presidential Policy Directive 21* establishes national policy to strengthen the security and resilience of critical infrastructure and states that the federal government shall work with critical infrastructure owners and operators to do so. DHS's Office of Cybersecurity and Communications, within the National Protection and Programs Directorate, leads this coordination for the communications sector as the sector-specific agency, and this office works with the Communications Sector Coordinating Council and the Communications Government Coordinating Council to set goals, objectives, and activities

[14] 47 U.S.C. §§ 151 et seq.

[15] As part of its programs on reliability and security, FCC also requires 911 service providers to take reasonable measures to provide reliable 911 service. 47 C.F.R. §12.4(c). These requirements were outside the scope of this review.

[16] 47 C.F.R. § 4.9. According to FCC, this outage data are presumed to be confidential and protected from routine public disclosure given their sensitive nature to both national security and commercial competitiveness.

for the sector.[17] During a national emergency or disaster, DHS also coordinates response efforts for communications systems in its role as the coordinator for Emergency Support Function #2 – Communications (ESF-2).[18] Specifically, two DHS components—the Federal Emergency Management Agency (FEMA) and Office of Cybersecurity and Communications—lead the federal government's work to support the restoration of communications infrastructure, coordinate response efforts, and facilitate the delivery of information to emergency-management decision makers.[19] DHS has direct access to FCC's NORS and DIRS data to support its work. Other DHS components also have responsibilities related to wireless network resiliency. For example, the Science & Technology Directorate conducts research in the area of wireless and other communications network resiliency, although its focus is on communications for the public-safety community.

Within the Department of Commerce, NIST also plays a role in promoting network resiliency by sponsoring the Community Resilience Panel. According to NIST, the Community Resilience Panel is sponsored by NIST and co-sponsored by other federal agencies to promote collaboration among stakeholders to strengthen the resiliency of infrastructure that communities rely on, including communications infrastructure.[20] As part of this mission, the panel seeks to identify policy and standards-related impediments to community resiliency, raise

[17] *Presidential Policy Directive 21* also notes that FCC is to partner with DHS and other agencies as appropriate on (1) identifying and prioritizing communications infrastructure, (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities, and (3) working with stakeholders to increase the security and resilience of the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure.

[18] The *National Response Framework* identifies 14 emergency support functions, broken out by functional area like communications or energy, that serve as the federal government's primary coordinating structure for building, sustaining, and delivering response capabilities. DHS, *National Response Framework Third Edition* (Washington, D.C.: June 2016).

[19] In addition to communications, energy, which includes commercial power, is another critical infrastructure sector. As such, it is also subject to similar oversight from DHS and its sector-specific agency, the Department of Energy.

[20] These agencies include the Department of Housing and Urban Development; Commerce's National Oceanic and Atmospheric Administration; DHS's FEMA and the Office of Infrastructure Protection; the Environmental Protection Agency; and the National Academies of Sciences, Engineering, and Medicine.

awareness of sector dependencies and of the cascading effects of disasters, and identify potential resiliency metrics.

Wireless Outages Caused by Physical Incidents Have Increased since 2009, and Outages due to Natural Disasters Lasted Longest

Trends in Number and Reported Causes of Wireless Outages

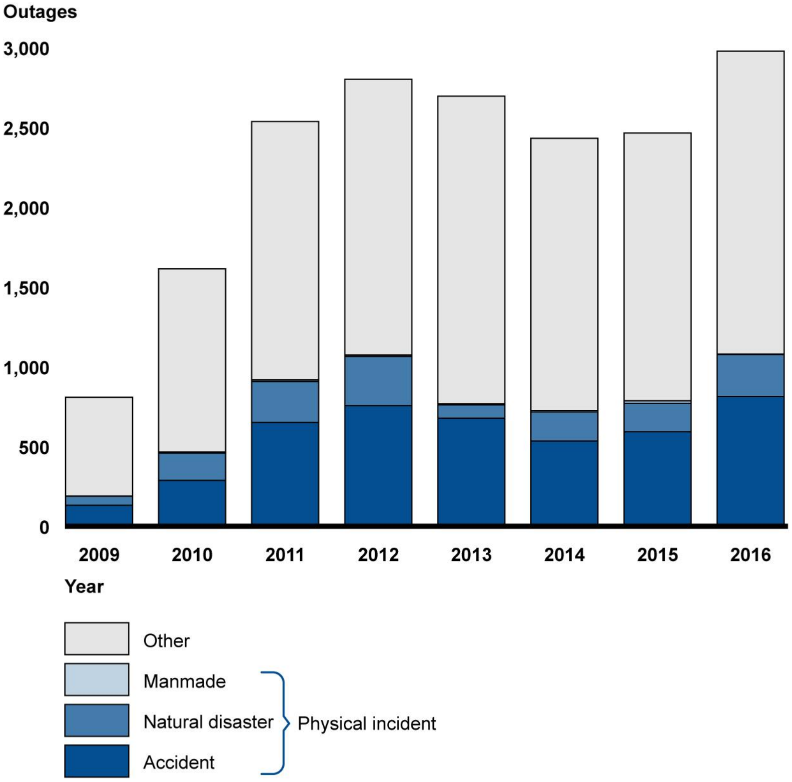
The number of wireless outages attributed to a physical incident increased from 2009 to 2016 (see fig. 2). Specifically, the number of outages with a physical incident reported as a root cause increased from 189 outages in 2009 to 1,079 in 2016.[21] The number of outages increased substantially during the first few years of this period and then was relatively stable, which mirrored the trend for all wireless outages. According to FCC officials, the increase in reported outages was due to increases in both the number of wireless customers and wireless infrastructure over this period, as well as due to FCC's outreach to wireless companies to clarify the thresholds for which carriers are required to report wireless outages to help ensure that carriers were consistently and fully reporting outages.[22] From 2009 to 2016, about one-third of all wireless outages reported to FCC (6,002 of 18,325) were attributed to physical incidents.[23]

[21] We primarily used the reported root cause to determine the cause for each wireless outage in this section, unless otherwise noted. The root cause is the underlying reason why an outage occurred or was reportable and is the key problem, which once identified and corrected, will prevent the same or a similar problem from recurring, according to FCC's NORS glossary. When reporting an outage, a wireless carrier is supposed to select the best fitting root cause from a list of options. Appendix I provides further information on how we identified outages attributed to physical incidents using the root cause field.

[22] For example, one threshold for which carriers are required to report a wireless outage is that the outage potentially affects at least 900,000 user minutes (e.g., affects 100,000 individual users for 9 minutes). 47 C.F.R. § 4.9(e).

[23] The other two-thirds of wireless outages that occurred during this period were attributed to other factors, such as planned maintenance to upgrade a network or equipment failures (e.g., a failed circuit card). See appendix II for more information on the trends in and characteristics of all wireless outages that occurred from 2009 to 2016.

Figure 2: Number of Reported Wireless Outages and Wireless Outages with a Physical Incident as the Root Cause, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

Note: “Other” includes outages caused by planned maintenance to upgrade a network or equipment failure (e.g., a failed circuit card).

Hurricane Maria

Hurricane Maria made landfall in Puerto Rico and the U.S. Virgin Islands only 2 weeks after Hurricane Irma, compounding damage to wireless networks and other infrastructure. The storm, which had sustained winds of nearly 175 miles per hour before it made landfall, severely damaged many roads, homes, and utilities. After landfall, Puerto Rico faced extensive power outages and limited communications capabilities. The President issued a disaster declaration for Puerto Rico and the U.S. Virgin Islands, and to support response and recovery from the hurricane, FEMA reported that more than 19,500 civilian personnel and military service members were on the ground in both locations.

Communications networks, including wireless networks, were significantly impacted by Hurricane Maria. In the days immediately following the hurricane's landfall, wireless carriers reported that 95 percent of cell sites in Puerto Rico were out of service, while over 65 percent of cell sites in the U.S. Virgin Islands were out of service. Given the scale of damage, 2 weeks later, about 85 percent and 60 percent of cells sites were out of service in these locations, respectively. FCC reported that wireless carriers deployed mobile cell sites (called cells on wheels and cells on light trucks) in Puerto Rico to help provide service. In addition, four wireless carriers opened up roaming on each other's networks to provide the maximum service possible and worked to coordinate repair work and placement of temporary assets to maximize the coverage for all subscribers.

Source: GAO based on FCC and other government reports. | GAO-18-198

Of wireless outages reported to FCC that were attributed to physical incidents, most were due to accidents, described below:

- Accidents—which include cable damage due to a backhoe cut, among other causes—were the root cause for 74 percent of wireless outages attributed to a physical event.
- Natural disasters—including tornados and wildfires—were the root cause for 25 percent of wireless outages attributed to a physical incident.
- Manmade events—which include damage associated with theft or other intentional damage to facilities—were the root cause for the remaining 1 percent of these outages.[24]

FCC typically suspends NORS reporting requirements in areas where FCC activates DIRS reporting for an emergency event, generally a natural disaster. For example, when FCC activated DIRS reporting for all counties in Puerto Rico and the U.S. Virgin Islands in response to Hurricane Maria in September 2017, FCC suspended NORS reporting requirements for those counties. As a result, FCC officials said that NORS data can undercount the number of wireless outages due to natural disasters. For a large natural disaster, however, FCC still can receive NORS reports for wireless outages outside the DIRS reporting area that are due to the natural disaster.

Looking beyond root cause reported for wireless outages, accidents remain the most common type of physical incident causing a wireless outage. Though root cause represents the underlying reason for an outage, FCC officials said an outage is often due to multiple events, so wireless carriers report a root cause and direct cause and can report two contributing factors when submitting information for an outage. Therefore, to better understand the number of outages linked to a physical incident, we looked at the number of outages citing a physical incident in any of the

[24] FCC's NORS data also includes a field where carriers report whether an outage was related to a malicious physical event. On average, carriers reported that 16 outages each year (less than 1 percent) were related to a malicious physical event.

cause and contributing factor fields.[25] Looking across cause fields, wireless outages citing an accident were most common, particularly from 2010 to 2016, as shown in figure 3. Wireless outages citing a natural disaster were less common, although there were several spikes in the number of outages citing a natural disaster. Some of these spikes correspond with major natural disasters like the derecho affecting Midwest and Mid-Atlantic states in 2012 or Hurricane Matthew in 2016.[26] Manmade events were rarely reported as the cause or contributing factor.

Hurricane Irma

In September 2017, Hurricane Irma made landfall as a Category 3 hurricane in Florida, having previously tracked near Puerto Rico and the U.S. Virgin Islands. The hurricane produced sustained winds of nearly 115 miles per hour as it made landfall in Florida. In the days that followed, the hurricane's impact was felt over the southeastern United States, with nearly 16 inches of rain falling over portions of Florida and high winds observed in five states. The President issued disaster declarations covering portions of Puerto Rico, the U.S. Virgin Islands, Florida, and Georgia.

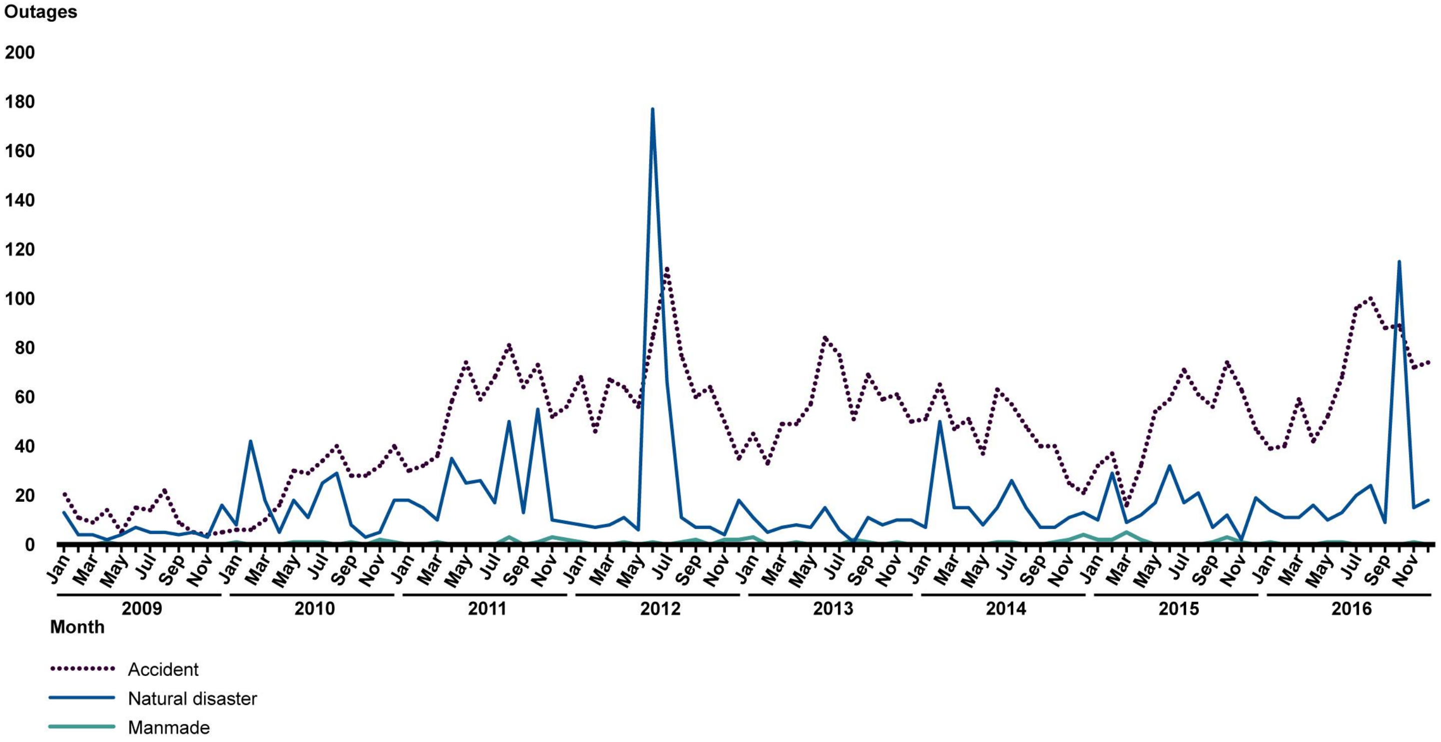
The damage from Hurricane Irma—both damage to wireless network infrastructure and damage resulting in power outages—created wireless service disruptions and outages in certain impacted areas. In particular, over half of cell sites were out of service for 3 or more consecutive days in five counties in Puerto Rico and in two counties in the U.S. Virgin Islands, according to data from wireless carriers reported to FCC. Within a week, only 6 percent of cell sites were out of service in reporting counties in Puerto Rico, but a majority of cell sites remained non-operational in the U.S. Virgin Islands; in one county, St. John, 90 percent of cell sites remained out of service a week and a half after landfall. In southern Florida, three counties had more than half of cell sites out of service for 4 straight days. The number of out-of-service cell sites decreased over time, so that less than 20 percent of cell sites were out of service in these counties within a week. Looking more broadly across all counties for which FCC collected data in Florida, Georgia, and Alabama, about 13 percent, 2 percent, and 1 percent of cell sites in the reporting area were out of service 4 days after Hurricane Irma's landfall, respectively.

Source: GAO based on FCC and other government reports. | GAO-18-198

[25] According to FCC's NORS glossary, the direct cause is the immediate event that results in an outage and is the event, action, or procedure that triggered the outage, and contributing factors are problems or causes that are closely linked to an outage. This paragraph and figure 3 describe the number of wireless outages, by month, that cited a natural disaster, accident, or manmade event in at least one of the cause or contributing factor fields.

[26] According to the National Weather Service, a derecho is a widespread, long-lived wind storm that is associated with a band of rapidly moving showers or thunderstorms.

Figure 3: Number of Reported Wireless Outages for Which a Physical Incident Was Cited as a Cause or Contributing Factor by Month, 2009–2016



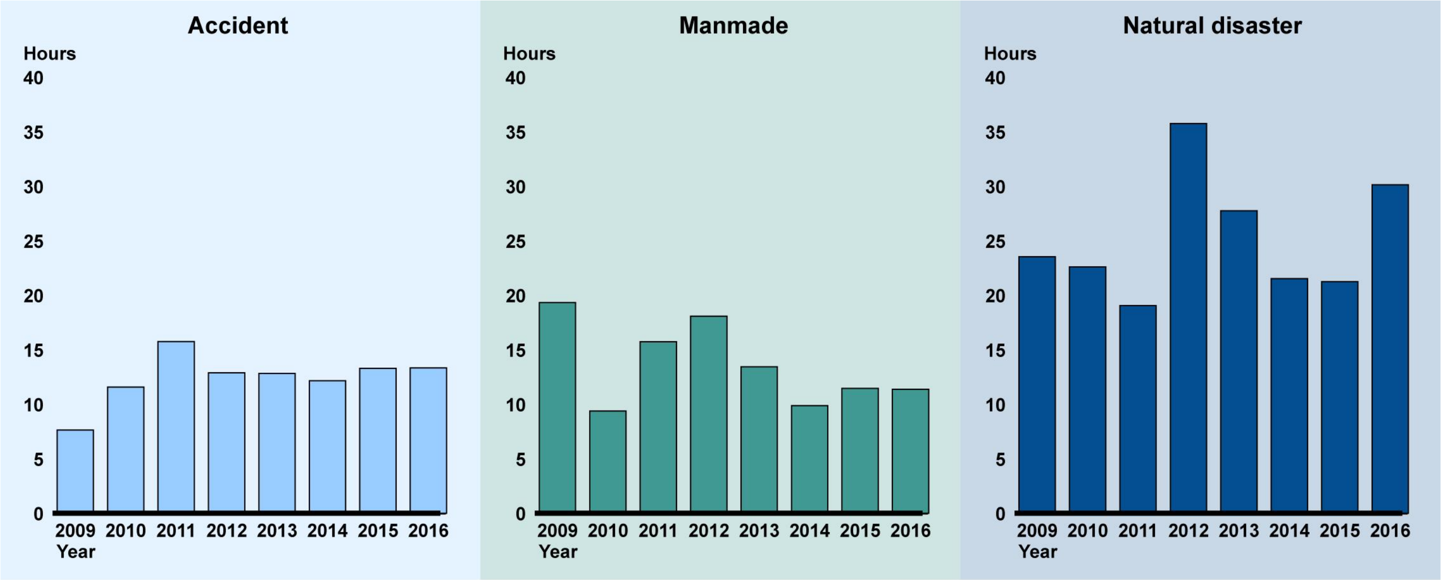
Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

Note: This figure shows the monthly number of wireless outages that cited a natural disaster, accident, or manmade event in at least one of the cause or contributing-factor fields.

Duration of Wireless Outages Attributed to Physical Incidents

While less common than accidents, wireless outages attributed to natural disasters lasted much longer than outages attributed to other physical incidents. Specifically, figure 4 shows that outages where a natural disaster was cited as the root cause were often twice as long as outages attributed to an accident or manmade event. From 2009 to 2016, the annual median duration of wireless outages attributed to accidents ranged from 8 hours to 16 hours, compared to natural disasters, which ranged from 19 to 36 hours.[27] Due to this longer duration, wireless outages attributed to natural disasters have a greater impact on the public as it is left without key means of communication for longer periods of time. In addition, an industry association told us that even though public safety officials primarily use dedicated communication networks, like land mobile radio networks, to carry out their work, they also rely on their mobile devices that use commercial wireless networks for maps and other applications.[28]

Figure 4: Median Duration of Reported Wireless Outages due to a Physical Incident, in Hours, by Root Cause, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

Note: Accidents include outages caused by cable damage due to digging or locating errors and damage associated with a vehicle accident. Natural disasters include outages caused by tornados, wildfires, and earthquakes. Manmade includes outages caused by damage associated with theft or another malicious act.

[27] Outages attributed to a power failure also had a relatively long median duration—the median duration for outages attributed to power failure ranged from 13 to 26 hours from 2009 to 2016.

[28] DHS administers the Wireless Priority Service program that authorizes communications providers to prioritize calls made over wireless networks by public safety officials and other priority users following a disruption of service.

Ten of 24 stakeholders we interviewed said that natural disasters pose the greatest risk to wireless networks as they have the most intense consequences.[29] Natural disasters can result in physical damage to or flooding of critical network components, and fallen trees and debris can temporarily block transportation routes, keeping repair crews from inoperable cell sites and other network components, as described in the *Community Resilience Planning Guide for Buildings and Infrastructure Systems*. Further, the failure of other systems like commercial power upon which wireless networks depend can lead to cascading failures in communications networks.[30] One industry association we spoke with said that natural disasters are the primary risk to wireless network resiliency as these events usually create the largest outages with the longest durations.

Hurricane Harvey

Hurricane Harvey made landfall as a Category 4 hurricane in Texas in August 2017 bringing record-breaking rainfall and strong winds to communities in its path. In the week following landfall, 30 to more than 40 inches of rain fell over thousands of square miles in the week that followed. The President issued a disaster declaration for over 40 counties in the area.

According to data from wireless carriers reported to FCC, some counties experienced a high number of out-of-service cell sites, a situation that can lead to limited service coverage or capacity. In four counties, more than 40 percent of cell sites were out of service for 3 straight days. The number of out-of-service cell sites decreased over time, so that less than 20 percent of cell sites were out of service in each of these counties within one week. Other counties in Texas and Louisiana had a much lower percentage of out-of-service cell sites, and across all counties, about 4 percent of cell sites were out of service in the week following the hurricane's landfall.

Source: GAO based on FCC and other government reports. | GAO-18-198

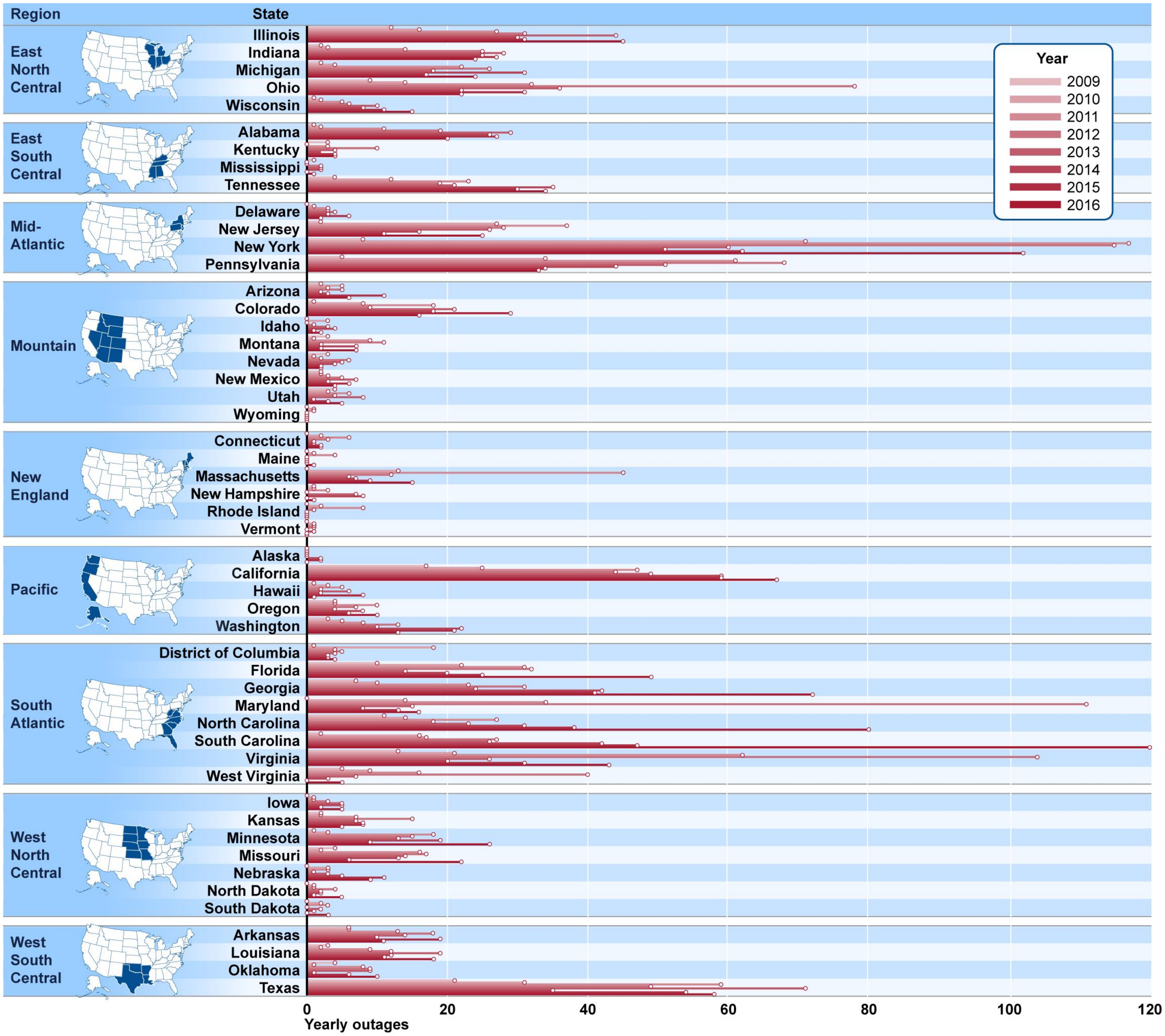
Location of Wireless Outages Attributed to Physical Incidents

By location, the number of wireless outages attributed to physical incidents increased from 2009 to 2016 in some states, including several of the most populous states such as California and Texas (see fig. 5). Most of the recent expansion of wireless networks has tended to be in the most populous states, as those states contain the most customers and the highest densities of customers, according to FCC officials. In addition, the thresholds for which carriers are required to report wireless outages in NORS are such that many outages that affect primarily rural areas will not accumulate enough user minutes to be reportable. However, the number of wireless outages with a physical incident as the root cause was relatively steady in many states or had spikes that generally corresponded with major natural disasters like the 2012 derecho.

[29] We asked all stakeholders to comment on the types of physical risks facing wireless networks and whether any type posed a greater risk. The remaining stakeholders did not identify a primary risk or rank the types of physical risks.

[30] U.S. Department of Commerce, *NIST Special Publication 1190: Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume I and II* (Washington, D.C.: May 2016).

Figure 5: Number of Wireless Outages with a Physical Incident as the Root Cause, by State and Region, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

For more detailed information on the location of all reported wireless outages that occurred from 2009 through 2016, including the cause and number of users associated with these outages, see an interactive graphic which can be viewed at http://www.gao.gov/products/gao-18-198.

Wireless Network Dependencies

Power failures and failures in other providers' networks (e.g., backhaul) played a role in the majority of wireless outages attributed to physical incidents. When an accident, natural disaster, or manmade event was the root cause for an outage, we found that wireless carriers often also reported a failure in one of these two key dependencies for wireless networks:

- Regarding power, 8 percent of wireless outages with a physical incident as the root cause (465 of 6,002 outages) cited power failure as the direct cause of the outage.[31] Nearly all these outages were attributed to a natural disaster.
- Regarding failures in other providers' networks, 87 percent of outages attributed to a physical incident (5,206 of 6,002 outages) were due to a failure in another provider's network, which includes backhaul connecting cell sites to mobile switching centers and onto the broader network. Most of these outages—4,111—cited an accident (i.e., a digging error resulting in cable damage) as the root cause. In 2014, a working group from an FCC-chartered federal advisory committee concluded that there is little to no shared, last-mile transport infrastructure for backhaul that wireless carriers (or other providers) could share dynamically to mitigate the effect of a backhaul failure. Thus, a backhaul outage will often result in a wireless outage. However, the working group identified existing best practices that providers can employ to help reduce or lessen the impact of failure in last-mile backhaul.[32]

[31] Conversely, of wireless outages with power failure as the root cause, 40 percent (554 of 1,390 outages) listed an environmental event as the direct cause, further demonstrating the relationship between natural disasters and power outages in causing wireless outages. See appendix II for more on reported root and direct causes for all wireless outages from 2009 to 2016.

[32] Communications Security, Reliability, and Interoperability Council, *Infrastructure Sharing During Emergencies, Transport Subcommittee, Shared Services* (Washington, D.C.: December 2014).

Federal Agencies and Industry Have Taken Some Actions to Improve Wireless Network Resiliency, but FCC's Oversight of Industry Actions Is Limited

Federal Agencies Largely Continue to Use Existing Mechanisms to Improve Resiliency

Since 2013, FCC and DHS have both continued to take action using a range of existing mechanisms to improve wireless network resiliency. These mechanisms include leading communications-specific planning activities and topic-specific research to develop and to share best practices. While these mechanisms are not new, FCC and DHS report updating and adapting these activities based on emerging needs and lessons learned from exercises and emergency events. FCC and DHS actions include the following:

- *Chartering advisory committees that examine resilience*: DHS and FCC charter federal advisory committees that have studied how agencies and industry could improve resiliency. For example, one such committee is FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), whose members include representatives from wireless carriers and other communications companies, industry associations, and federal, state, and local agencies. CSRIC working groups often develop best practices for industry and make recommendations to wireless carriers, FCC, and others to improve network resiliency. One example is a working group that studied how industry could share backup power resources in 2014. FCC maintains a database of best practices and publicizes these through presentations at conferences and in public reports, as it did in a report on communications outages caused by the 2012 derecho. Six stakeholders we interviewed said best practices represent a valuable means to improve resiliency, as for example, best practices are flexible and enable providers to adapt practices as communications networks evolve. One stakeholder attributed CSRIC's effectiveness in issuing and promoting best practices and information in part to its affiliation with the industry's regulator, FCC. Other advisory committees that examined resiliency include DHS's National Security Telecommunications Advisory Committee and FCC's Technological Advisory Council.

- *Developing and implementing procedures to respond to physical incidents*: DHS leads emergency communications response and recovery efforts, as coordinator for ESF-2. For example, within DHS, the National Coordinating Center for Communications (NCC) holds weekly calls with government and industry partners to exchange information as part of NCC's work to continuously monitor events that may affect communications.[33] These weekly calls sustain relationships and promote readiness that can be leveraged to coordinate a response to an emergency incident, according to DHS and FCC officials and members of the Communications Sector Coordinating Council. During an incident, NCC reports that it holds these calls on a daily basis to understand the status of wireless and other networks—along with FCC outage data and other information collected from carriers—and to support industry response efforts. For instance, NCC officials said that during an incident they can help carriers find available generators or work with local governments to enable carriers to enter disaster areas to make repairs if carriers are denied access. Two carriers we interviewed said the NCC works well to support industry response to and recovery from incidents, as NCC has established response processes to help the communications sector to coordinate with the power industry. According to DHS, NCC participates in the Energy Priority Restoration Group that is dedicated to determining power restoration priority following an incident.[34] While this group includes many sectors, it enables communications providers to help prioritize power restoration for critical communications components, like mobile switching centers.[35]
- *Analyzing wireless outage data to identify trends and areas for further study*: As noted above, FCC collects and regularly analyzes data on wireless outages during the regular course of business and during emergency events. FCC meets with each nationwide wireless carrier annually to discuss trends in the carrier's outages and any issues related to how the carrier completes NORS reports, according to FCC officials and an industry association we interviewed. FCC also analyzes and shares its analysis of NORS data with industry at

[33] According to DHS, 11 federal government agencies (including FCC) and over 60 private-sector-communications and information-technology companies (including major wireless carriers) routinely share critical communications information and advice to support the NCC's mission.

[34] This group is part of the emergency support function for the energy sector.

[35] To further improve this coordination, FEMA is finalizing a Power Outage Incident Annex to supplement existing national response and recovery plans.

quarterly meetings of the Alliance for Telecommunications Industry Solutions' Network Reliability Steering Committee.[36] Specifically, FCC presents trends in NORS outage data for the last 3 years for different types of outages. Such data include trends in the total number and duration of wireless outages. The Network Reliability Steering Committee, at FCC's request or its own initiative, establishes teams to examine NORS trends and to make recommendations that may increase network reliability and reduce network outages.[37] Based on this work, the team may identify relevant best practices that carriers could use to reduce or eliminate outages or suggest refining or creating a new best practice. Representatives from two industry associations said that FCC meets with industry to discuss outage data and is receptive to feedback on how to improve data-reporting processes and data quality.

In addition to these existing mechanisms, federal agencies have initiated some new activities to enhance wireless network resiliency since 2013.

- *Community Resilience Panel*: NIST issued the *Community Resilience Planning Guide for Buildings and Infrastructure Systems* in October 2015 and sponsors the Community Resilience Panel, which aims to reduce barriers to achieving community resilience by promoting collaboration among stakeholders to strengthen the resilience of buildings, infrastructure, and social systems upon which communities rely. The panel held its first meeting in November 2015.[38] The planning guide provides a process that communities can use to improve their resilience by setting priorities and allocating resources to manage risks based on their prevailing hazards. The guide also devotes sections to key infrastructures; the communications section

[36] The Alliance for Telecommunications Industry Solutions is a global standards development and technical planning organization that supports the creation and adoption of international technical and operational standards for information, entertainment, and communications technologies. Its Network Reliability Steering Committee provides consensus-based technical and operational guidance and best practices to help ensure the reliability of communications networks. This committee provides feedback to FCC on NORS and DIRS, among other efforts.

[37] The Alliance for Telecommunications Industry Solutions maintains a list of industry best practices at http://www.atis.org/bestpractices/Default.aspx. This list matches FCC's best practice database.

[38] The panel has more than 350 members and membership is open to anyone with an interest in community resilience. Members include representatives from private companies, including communications companies; universities; local governments; and federal agencies.

describes components of communications networks, the regulatory environment, and industry standards that can help inform community planning. The Community Resilience Panel also has a Communication Standing Committee comprised of industry and government members. This committee is currently creating additional resources to support communities, including a methodology that communities could use to involve wireless carriers and other communications providers in resilience planning activities. While communities have started to use the guide, NIST officials said it is too soon to measure or point to specific outcomes attributable to the Community Resilience Panel's work.

- *Post Hurricane Sandy hearings and proposed rule*: In 2013, FCC held field hearings on network reliability and continuity. The goals of the hearings were to improve network resiliency, improve restoration, empower the public, and unleash technological solutions. The two hearings included a wide range of panelists including representatives from FCC and FEMA, state and local agencies, consumer groups, wireless carriers, and other communications providers. Following the hearings, FCC issued a notice of proposed rulemaking to promote transparency to the public on how wireless carriers compare in keeping their networks operational during emergency events. Specifically, FCC's proposed rule would publicly report the number and percentage of each carrier's cell sites that remained operational during an emergency event to enable consumers to compare wireless carriers when purchasing service.[39] Based on our review of comments, public safety and consumer groups tended to support the proposed rule while industry expressed concerns, in particular, that the public reporting in the proposed rule would not accurately portray the service available during an emergency or be a useful measure to help consumers choose among wireless carriers. FCC decided not to issue a final rule, stating in December 2016 that a voluntary industry approach, described below, provided a more appropriate path to improve network resiliency.[40]

We asked stakeholders about the results of the actions taken by FCC and DHS, and across the 24 stakeholders we interviewed, there was no consensus regarding needed improvements in DHS and FCC guidance,

[39] *In the Matter of Improving the Resiliency of Mobile Wireless Communications Networks*, 28 FCC Rcd 14373 (2013).

[40] *In the Matter of Improving the Resiliency of Mobile Wireless Communications Networks*, 31 FCC Rcd 13745 (2016).

coordination, or research on wireless resiliency.[41] Seven stakeholders said they did not think there were any gaps or needed improvements from FCC, and six stakeholders said they did not think there were any gaps or needed improvements from DHS. Although most stakeholders identified a need for further federal agency action, they tended to identify dissimilar actions. However, the three state and two local agencies we interviewed noted that more real-time data on wireless outages would help aid their efforts to respond to an incident, which we discuss further below.

Voluntary Industry Framework Aims to Improve Wireless Network Resiliency, but FCC Has Limited Plans to Monitor This Framework

In April 2016, an industry coalition consisting of CTIA, a wireless industry association, and five wireless carriers announced the Wireless Network Resiliency Cooperative Framework (framework) in response to FCC's 2013 notice of proposed rulemaking on wireless network resiliency.[42] The framework is a voluntary initiative designed to advance wireless service continuity and information sharing during and after emergencies by enhancing coordination and communication, both among carriers and between carriers and government.

The framework has five elements; some elements are specific to disaster response while other elements focus on preparedness and education. Industry has taken steps related to all five elements of the framework, as described in table 1. Furthermore, CTIA representatives told us they have ongoing meetings with representatives from the public-safety community, the outcome of which they expected to be a series of best practices concerning planning before disasters, addressing coordination during and after emergencies, and developing education and awareness strategies in fall 2017. The threshold to trigger the response elements is when DHS activates ESF-2 and FCC activates DIRS. At the time of our review, four events—Hurricane Matthew in October 2016 and hurricanes Harvey, Irma, and Maria in late 2017—had met the threshold to trigger the

[41] We did not ask stakeholders about guidance or research from NIST because its *Community Resiliency Planning Guide for Buildings and Infrastructure Systems* was recently issued and its resilience work does not focus solely on the communications sector.

[42] The carriers were AT&T, Sprint, T-Mobile, US Cellular, and Verizon.

response elements.[43] Prior to the three events in 2017, FCC officials and three stakeholders we interviewed told us it was too soon to know the effectiveness or results of the framework.[44]

Table 1: Description of and Steps Taken to Implement the Wireless Network Resiliency Cooperative Framework, as of October 2017

Element	Description	Steps taken
Response elements		
Providing for roaming under disasters	Wireless carriers commit to working with one another to implement roaming arrangements for the duration of an event. Roaming would occur when a requesting carrier's network is inoperable (after taking steps to restore the network), when roaming is technically feasible, and when the roaming will not adversely affect the non-requesting carrier's network.	Two of the signatory wireless carriers implemented roaming arrangements during Hurricane Matthew (2016). Following Hurricane Maria (2017), the Federal Communications Commission (FCC) reported that four wireless carriers had opened up roaming in Puerto Rico so that they could collectively serve the maximum population of the islands with the current coverage available. This included both signatory and non-signatory wireless carriers.
Fostering mutual aid	Wireless carriers commit to establish mutual aid arrangements with one another to provide aid, such as sharing physical assets, during and after an event.	According to FCC, some national carriers implemented mutual aid arrangements during Hurricane Matthew, Hurricane Irma (2017), and Hurricane Maria. For example, one carrier allowed another carrier to use its facilities in the U.S. Virgin Islands during Hurricane Irma.
Improving public awareness regarding service and restoration	Wireless carriers will support FCC making data on the number of out-of-service cells sites, aggregated across carriers, publicly available. Data will be posted for counties covered by an FCC Disaster Information Reporting System (DIRS) activation notice.	FCC posted daily data on the number of out-of-service cells sites by county for 8 days for Hurricane Matthew, 11 days for Hurricane Harvey (2017), 12 days for Hurricane Irma, several weeks for Hurricane Maria, and 1 day for Hurricane Nate (2017).[a]
Preparedness and education		
Enhancing municipal preparedness and restoration	Wireless carriers will convene select local governments' public safety representatives to develop best practices to facilitate coordination before, during, and after events to maintain and restore wireless service. Wireless carriers will also provide contact information for a carrier/public safety answering point database, to be made available to a state emergency operations center during an event.	CTIA, a wireless industry association, convened a working group that includes officials from state and local governments, according to CTIA representatives. The working group is carrying out its work to identify best practices in three sub-groups: (1) pre-event planning, (2) coordination during and after an event, and (3) education and awareness.

[43] Industry also implemented two of the response elements of the framework—roaming under disasters and mutual aid—during flooding in Louisiana in August 2016, though this event did not meet the threshold to trigger the framework.

[44] In October 2017, FCC announced that it would form an internal task force to support the restoration of communications services affected by the 2017 hurricane season with a particular emphasis on addressing challenges in Puerto Rico and the U.S. Virgin Islands.

Element	Description	Steps taken
Increasing consumer readiness and preparation	Wireless carriers will conduct consumer education to ensure consumers are properly prepared for emergencies and disasters. In particular, CTIA will develop a Consumer Readiness Checklist and strategies to disseminate the checklist.	CTIA created a website titled How to Prepare Wireless Devices for Emergencies that includes a video and list of steps for consumers to take to prepare for an emergency.[b] Select carriers have also issued press releases to consumers, for example, on carrier and consumer efforts to prepare for hurricane season.

Source: GAO review of FCC documents, CTIA documents, and interviews. | GAO-18-198

Note: The response elements are triggered by an emergency or disaster for which (1) the Federal Emergency Management Agency activates Emergency Support Function 2, and (2) FCC activates DIRS.

[a] FCC posted data for each event at a dedicated website—https://www.fcc.gov/matthew, https://www.fcc.gov/harvey, https://www.fcc.gov/irma, and https://www.fcc.gov/maria. The posted data were submitted by the five signatory carriers to the framework and several companies that agreed to allow FCC to include their data. FCC officials noted that for Hurricane Irma, four carriers that provide service to Puerto Rico and the U.S. Virgin Islands all agreed to allow FCC to use their data in the aggregated data.

[b] The CTIA website is at https://www.ctia.org/consumer-tips/emergency-preparedness-wireless-tips.

FCC is responsible for administering policies to improve resiliency, which include monitoring actions taken by industry, and federal standards for internal control state that management should establish and operate monitoring activities, evaluate and document the results of ongoing monitoring, and then identify changes that either have occurred or are needed.[45] Federal standards for internal control also state that agencies should define objectives clearly and that objectives should be in specific and measurable terms that allow for the assessment of performance.[46]

In December 2016, FCC said it would continue to engage with industry on the implementation and use of the framework, and FCC has taken some steps to monitor the framework's implementation. Specifically, FCC developed a plan to track certain tasks related to the framework in August 2017. This plan

- tracks the completion of initial tasks related to the framework, such as tracking industry's publication of best practices to enhance municipal preparedness and resiliency, and confirming the five signatory wireless carriers' commitment to the framework, and
- notes that FCC will update its emergency response documents to ensure that the documents reflect the framework and include

[45] GAO-14-704G.

[46] GAO-14-704G.

checklists to validate that carriers take these actions during emergency events (e.g. instituting roaming, providing mutual assistance).[47]

In August 2017, FCC also issued a public notice inviting carriers beyond the five signatory wireless carriers to sign on to the framework.

However, we found FCC's plan does not include any steps to document and assess the effect of the framework on the resiliency of wireless networks. In particular, FCC's plan does not track any outputs or outcomes over time that speak to the results of the framework, such as the number of roaming requests made and fulfilled during an emergency event.[48] FCC's plan to monitor the framework is still new. According to FCC officials, FCC did not decide what division would lead its monitoring of the framework until August 2017 because it needed to determine which division should have responsibility for the framework.[49] Since the plan was created, FCC has met with industry groups and individual carriers to gather additional information and has updated its plan with this information to track implementation tasks.

Overall, by monitoring the outputs and outcomes of the framework, FCC could determine where further changes are needed to help ensure that wireless networks are resilient. In 2016, FCC reported that the framework could produce benefits such as bolstering FCC's situational awareness and providing consumers with a means to hold carriers accountable for service continuity during emergency events. Yet, seven stakeholders we interviewed, including wireless carriers, said the framework largely codified actions that carriers already generally take to prepare for and respond to an emergency event. In addition, comments submitted to FCC in 2016 were split on whether the framework represented a sufficient path

[47] In particular, FCC plans to update its Incident Management Plan, used leading up to and during emergencies, following the 2017 hurricane season. In addition to reflecting the framework, FCC officials said the update will incorporate lessons learned from hurricanes Harvey, Irma, and Maria. FCC officials said it is also participating in DHS's efforts to update the ESF-2 concept of operations document.

[48] Outputs can be defined as the direct products and services delivered by a program or initiative, while outcomes are the results of those products and services.

[49] Specifically, FCC officials said the framework was initially the responsibility of the Cybersecurity and Communications Reliability Division with support from the Office of Emergency Management; in August 2017, FCC transitioned full responsibility for the framework to the Cybersecurity and Communications Reliability Division.

forward, and some stakeholders noted specific issues that they believed could limit the effectiveness of the framework, for example:

- Four stakeholders we interviewed—an industry association, local agency, state agency, and consumer group—cited the lack of federal agency enforcement or monitoring.
- Two industry associations stated in joint comments that there was no assurance that all carriers would conduct adequate testing to enable roaming under disasters.[50]
- A local agency said in comments that the threshold to trigger the response elements was too high; as such, carriers would not be-obligated to implement the elements for more local events.[51]

Therefore, monitoring the outputs and outcomes of the framework would help FCC understand the effect of industry formalizing these actions in the framework.

Furthermore, although FCC and industry documents that describe and endorse the voluntary framework include broad goal statements, there are no specific measures for what the framework hopes to achieve. As a result, FCC lacks specific and measurable terms to monitor the effect of the framework. The CTIA- and carrier-released public summary of the framework said it aims to advance wireless service continuity and information sharing during and after emergencies and disasters, as well as help consumers be better prepared for future disasters. FCC, when endorsing the framework, said it was a reasonable approach to achieve FCC's stated goals for the 2013 proposed rule, including promoting availability of wireless mobile services in the event of natural disasters and increasing provider transparency around wireless resiliency. FCC officials told us they have not discussed possible measures to monitor the

[50] In comments, the associations said that entering a roaming agreement requires negotiating the terms of the agreement and testing the roaming functionality on the involved wireless networks. According to these associations, which represent small and rural carriers, nationwide carriers only conduct unilateral testing for roaming agreements (i.e., that the other carrier's subscribers can use the nationwide carrier's network), as they often restrict their subscribers from roaming on the networks of smaller carriers. Therefore, in an emergency situation, the nationwide carrier's subscribers may not be able to roam on the other carrier's network as testing has not been conducted to ensure that roaming can occur.

[51] Since 2009, DHS had activated ESF-2 for 10 incidents, and FCC had activated DIRS for 11 incidents.

effect of the framework with industry participants. As the creators of the framework, industry participants could provide insight into such measures. However, FCC officials acknowledged that it will be important to determine what the results of the framework have been in light of the 2017 hurricanes, and that developing measures to assess industry's efforts under the framework would be beneficial.

In addition, FCC has not communicated the framework to all state and local public-safety officials and wireless carriers, potentially limiting its effectiveness. At the time of our review, CTIA and the signatory wireless carriers had released a high-level summary of the framework but no additional documentation on the scope of wireless carriers' obligations under the framework.[52] Based on our interviews, we found that knowledge of the framework was not widespread. Six stakeholders we interviewed, including representatives of state agencies we interviewed and a non-signatory wireless carrier, were either unaware of the framework or unaware of whether industry had taken actions on any elements of the framework since its announcement. For example, a state emergency manager in one state affected by Hurricane Matthew was unaware of the framework and that FCC, based on one element of the framework, had posted daily status updates on wireless service following the hurricane. This manager noted that those updates would be useful for response efforts.

Federal standards for internal control state that federal agencies should externally communicate necessary, quality information to achieve the agency's objectives and that open communication can also help enable a federal agency to obtain information from external parties.[53] Among the stated objectives of FCC is to advise and assist public safety entities on wireless communications issues and to develop and administer policy goals and plans to promote reliable communications for public safety and disaster management.[54] Moreover, one of FCC's current strategic objectives is to promote access to effective public-safety communications services used by government as well as all consumers in need. To address this and other objectives, FCC stated that it will facilitate

[52] *In the Matter of Improving the Resiliency of Mobile Wireless Communications Networks*, PS Docket 13-239, Ex Parte Presentation, CTIA et al. (2016).

[53] GAO-14-704G.

[54] 47 C.F.R. § 0.191 (a) and (f).

discussions and share information among key constituencies.[55] FCC uses several mechanisms and standing forums to share information and educate constituencies. For example, FCC gives presentations about FCC activities at conferences on public safety communications that include state and local officials.[56] In addition, FCC participates in the regular conference calls hosted by DHS's NCC through which government and industry exchange information and the Network Reliability Steering Committee's public quarterly meetings, as noted above.

Without greater awareness of the framework, state and local public safety officials may continue to be unaware of tools or other improvements available through the framework that could help them prepare for or respond to an emergency, such as the posting of daily updates on the number of out-of-service cell sites or best practices that could aid resilience. Also, smaller and rural (non-signatory) wireless carriers might be unaware of commitments made by the signatory carriers, such as committing to roaming under disasters that could benefit them and the citizens they serve during an emergency event but may require entering into and testing a roaming arrangement. By actively communicating information about the framework, FCC could also increase the likelihood of receiving information from industry or state and local public-safety officials about any implementation issues or positive results from the framework. In August 2017, FCC created a website that summarized the framework and, as noted above, issued a public notice inviting additional carriers to sign on to the framework. Only two carriers, as of October 2017, beyond the carriers involved in creating the framework publicly informed FCC of their intent to participate in the framework. As of October 2017, FCC officials told us they did not have additional plans to promote awareness of the framework, but noted that it would be important to inform relevant stakeholder groups about the framework, especially those who might remain unaware of it.

[55] *FCC Strategic Plan, 2015-2018*.

[56] For instance, FCC officials said they attend and present at conferences hosted by APCO International, an organization of public safety communications professionals, and the National Emergency Management Association, an association of the emergency management directors from states, territories, and the District of Columbia.

Stakeholders Cited Advantages and Disadvantages for Options Aimed at Improving Wireless Network Resiliency

We identified options that federal agencies could take to further improve wireless network resiliency based on agency reports, federal advisory committee recommendations, peer-reviewed literature, and other reports. The options we identified could be implemented either alone or in combination and are not meant to be exhaustive. We categorized them by their aim—preparedness, response, and awareness. FCC, as the regulator for wireless communications, would be the likely agency to implement many of the options, although DHS or other federal agencies could play a role in implementing some of the options. We asked stakeholders to comment on the advantages and disadvantages, including the feasibility—technical, legal, or other—of each option. The tables below describe identified options by category, along with the most frequently cited advantages and disadvantages.

FCC has previously suggested and discussed some of these options, most recently during its notice of proposed rulemaking in 2013. FCC noted that its proposed rule sought to comply with guidance from the Office of Management and Budget to use disclosure requirements or transparency measures where possible in place of prescriptive regulations. However, as noted above, FCC declined to issue a final rule, stating that the proposed rule was problematic in light of substantial concerns raised about proposed metrics and disclosure requirements.

Preparedness

Two options identified in agency reports and literature intend to improve resiliency by focusing on actions to be taken ahead of an emergency or disaster, as described in table 2.

Table 2: Preparedness Options to Improve Wireless Network Resiliency and Examples of Advantages and Disadvantages

Option description	Advantages cited by stakeholders	Disadvantages cited by stakeholders
Require wireless carriers to provide a minimum amount of backup power at cell sites or other critical communications facilities.[a]	Backup power would help mitigate the effects from wireless outages due to commercial power outages. Backup power requirements would help ensure continued service given the increased dependency of the public on wireless phone service for public safety. Public safety officials would know how long cell service would last during power outages if there were specific backup power requirements. Technological advances in backup power have made this requirement more feasible.	Not all cell sites are suitable for backup power (e.g., a cell site on a rooftop is subject to space and weight constraints) so a requirement could discourage carriers from deploying more cell sites, lowering network redundancy. This requirement could be costly and burdensome, and costs could be passed onto consumers. Long power outages (i.e., outages that exceed the minimum amount of backup power) would still likely lead to wireless outages. Several carriers and infrastructure owners already provide backup power at specific components, like macro cell sites that provide key coverage to an area, based on a particular network's needs. Zoning, permitting, and environmental protection rules make installing backup power difficult in some locations.
Issue guidance to states and localities regarding policies for siting or construction standards that would allow for easier deployment of telecommunications infrastructure, such as towers that host cell sites.	This option could address difficulties (cost and time) carriers and other infrastructure providers can face from inconsistent rules or rules that hinder deployment and thus could enable wireless carriers to deploy more sites to help make networks more resilient. This option was generally seen as cost effective when compared with other options (e.g., options that set new network requirements).	Since the implementation of this guidance would be left to states and localities, this option may have limited impact. There are concerns that guidance could lead to calls for federal rules to pre-empt state and local rules. Guidance may not be flexible enough to consider the different needs and vulnerabilities facing different states and localities; for example, different areas in the country are more at risk for earthquakes than other areas.

Source: GAO analysis of Federal Communications Commission (FCC), Department of Homeland Security, federal advisory committee, and other reports, and interviews of selected stakeholders. | GAO-18-198

[a] In 2013, FCC sought comments on options to improve wireless network resiliency in addition to its proposed rule to disclose the percentage of a carrier's cell sites that are operational during major emergencies. FCC suggested and sought comment on this option in its order but did not take any further action on this or other options when it closed the proceeding in 2016.

Twelve stakeholders we interviewed raised concerns about the feasibility of the option to require a minimum level of backup power at cell sites due to technical or legal issues. In 2007, FCC adopted a requirement for wireless carriers to provide 8 hours of backup power at cell sites. That requirement was vacated after the Office of Management and Budget disapproved the rule's information collection requirements. In contrast, nine stakeholders we interviewed were more positive about the feasibility of guidance. Further, FCC created the Broadband Deployment Advisory Committee in January 2017 to provide recommendations on how to accelerate broadband deployment. Two of the committee's five working groups focus on state and local regulatory barriers and model language for state and municipal code, both of which could provide a model for wireless network infrastructure.

Response

As shown in table 3, agency reports and literature also included options related to response activities during and after an emergency event.

Table 3: Response Options to Improve Wireless Network Resiliency and Examples of Advantages and Disadvantages

Option description	Advantages cited by stakeholders	Disadvantages cited by stakeholders
Require wireless carriers (and other communications providers like cable companies) to open Wi-Fi hotspots usually limited to a carrier's subscribers in emergency situations, or facilitate communities or other organizations to create resilient Wi-Fi networks.[a]	Wi-Fi hotspots can provide a lifeline to citizens, such as allowing them to obtain emergency information via the Internet and call 911. Wireless carriers have opened their Wi-Fi networks in prior emergency situations, enabling communications between citizens and public safety agencies. Communities could sponsor Wi-Fi hotspots to keep people connected during emergencies.	Opening Wi-Fi hotspots normally subject to authentication requirements could create network security concerns. Wi-Fi hotspots also rely on commercial power and thus may be unavailable during some emergency events. Wi-Fi hotspots could be prone to overloading. Wi-Fi would not be feasible to provide service in lower-density areas, since Wi-Fi signals have a limited range. Communities could face difficulties funding and maintaining community Wi-Fi networks in the long term.
Require wireless carriers to disclose information about service outages to local authorities with public safety duties.	Real-time outage information improves the situational awareness of first responders and allows them to identify where additional resources are needed, for instance, by informing them where citizens cannot reach 911 by wireless phones. The Federal Communications Commission (FCC) already collects some data on outages, such as FCC's Disaster Information Reporting System (DIRS) data, that could be used for this purpose. Information sharing would keep both the public safety community and public informed of the recovery process.	Industry is concerned about the potential release of sensitive, proprietary data. For instance, FCC treats outage data as confidential, and data shared with local public safety agencies could be obtained using open records laws in some jurisdictions. Requiring such disclosures could be costly and burdensome and could divert resources from restoring service to meeting disclosure requirements. Not all public safety groups would be able to process or interpret this information; for example, requiring such disclosures could potentially overwhelm a public safety agency if it lacked the capacity to handle the high volume of disclosures.

Source: GAO analysis of FCC, Department of Homeland Security, federal advisory committee, and other reports and interviews of selected stakeholders. | GAO-18-198

[a] Some but not all wireless carriers operate Wi-Fi hotspots, so this requirement would not apply to all carriers. Other communications providers, like cable providers, sometimes also operate Wi-Fi hotspots.

For the first option, FCC officials and six stakeholders we interviewed noted that wireless carriers have on occasion opened up their networks in prior emergency situations, which indicates that the option is technically feasible. For the second option, every state and local agency we spoke with noted the value of having real-time information on wireless outages during an emergency event. FCC collects DIRS data, and these data are confidential when provided to FCC. According to FCC, if outage data were shared with a state or local agency, it may be subject to open records laws that provide a means for the public to gain access to government documents.

Awareness

Other options are intended to improve wireless network resiliency by fostering transparency, as described in table 4. For some options below, transparency would involve making information publicly available so consumers could use this information when choosing a wireless carrier. Such transparency could give industry an incentive to improve the resiliency of their networks. For example, by setting performance standards or requiring wireless carriers to disclose their efforts to improve resiliency, consumers could compare the performance or practices of wireless carriers. However, some of these options would require defining specific parameters, whether a metric or the specific information to disclose, and seven stakeholders we interviewed noted this could be difficult given factors such as the variation in carriers’ wireless networks and the pace of technological change. For other options below, transparency would involve more selectively sharing information with other public safety agencies to improve coordination and aid planning for possible disruptions to wireless networks during emergencies.

Table 4: Awareness Options to Improve Wireless Network Resiliency and Examples of Advantages and Disadvantages

Option description	Advantages cited by stakeholders	Disadvantages cited by stakeholders
Require wireless carriers to report and disclose information about practices designed to promote network resiliency, such as extent of backup power and supplementary infrastructure a carrier can deploy to provide service.[a]	Information about carriers' response capabilities could assist public safety officials with emergency preparation processes. More data available to the public about resiliency practices taken by carriers could help consumers make informed choices when purchasing wireless service. Accurate information about network components, such as cell tower location and the points of interconnection for network-to-network coverage, could help facilitate and monitor roaming between carriers under disasters.	Industry is concerned about the potential release of business confidential and sensitive information to competitors or malicious actors. The public may not be able to understand or use the disclosed information on a carrier's practices. This disclosed information may lead to unfair comparisons between carriers, particularly between large and small or urban and rural carriers. This information is less useful to public safety agencies than real-time outage information.
Use crowd-sourced data to track the performance of wireless carriers in providing reliable, resilient service, specific to or including emergency and disaster events, and make the information publicly available.[a]	More data available could help consumers make informed choices based on the performance of carriers' networks. Using crowd-sourced data is less burdensome to carriers than requiring new data disclosures. Crowd-sourced data could be a useful tool for emergency management agencies as it provides a picture of where damage occurs and where to dispatch resources.	Stakeholders raised concerns about the accuracy, reliability, and completeness of crowd-sourced data. Consumers may not find the information useful or understandable. Data on network performance is currently available from commercial sources, which may make federal involvement unnecessary. Crowd-sourced data would not enable reliable comparisons across carriers of different types (e.g., nationwide and rural) or networks.
Design a reliability metric so federal agencies can track wireless network resiliency, based on existing data sources such as the Network Outage Reporting System (NORS) and Disaster Information Reporting System (DIRS), or on new data sources.	A resiliency metric would make it easier for government and consumers to track network resilience over time against a common benchmark.[b] Data gathered over time can help industry, government, and researchers improve forecasting, predictive modeling, and planning for wireless network outages.[b] Emergency managers could use this information to formulate disaster response plans.	It would be difficult to develop a simple metric that would be useful and remain relevant as technology changes. A metric would be of limited use if only for federal agency use and not for the public. Any new data collected for a metric would impose additional compliance costs on carriers.

Option description	Advantages cited by stakeholders	Disadvantages cited by stakeholders
Formulate and implement wireless network resiliency performance standards that establish minimum levels of network reliability, including incentives for achieving them or penalties for failing to achieve them.[a]	More consumers are depending on wireless networks as their primary or only means of communication, so setting minimum performance standards analogous to other utility services may be appropriate. Performance standards could ensure that wireless networks continue working during disasters. Performance standards could make it easier for consumers and others to compare carriers.	The competitive nature of the wireless industry already provides incentives for carriers to improve resiliency without performance standards; for instance, carriers already compete on resiliency, and the public indicates how much it values resiliency based on its willingness to purchase more resilient service. Performance standards would impose costs on carriers and the federal agency charged with enforcing the standards. Developing appropriate performance standards could be difficult, especially with changing technology.

Source: GAO analysis of Federal Communications Commission (FCC), Department of Homeland Security, federal advisory committee, and other reports and interviews of selected stakeholders. | GAO-18-198

[a] In 2013, FCC sought comments on options to improve wireless network resiliency in addition to its proposed rule to disclose the percentage of a carrier's cell sites that are operational during major emergencies. FCC suggested this option in its order but did not take any further action on this or other options when it closed the proceeding in 2016.

[b] In analyzing stakeholder responses, we identified only one advantage cited by multiple stakeholders; therefore, we also included advantages identified in federal agency and federal advisory committee reports.

Conclusions

During natural disasters and other emergencies, wireless network outages can make emergency communications, such as making 911 calls, nearly impossible for the vast number of people who rely solely on wireless communications. The wireless industry sought to enhance resiliency by improving the continuity of wireless service and information sharing during and after emergency events by introducing a voluntary framework. Although FCC stated that this voluntary framework would have many benefits, neither industry nor FCC has identified any specific, measurable objectives that could be used to determine whether the framework meets its broad goals, and FCC has limited plans to monitor the framework's implementation and use. Absent sufficient monitoring, including identifying specific, objective measures for the framework, FCC lacks information on the framework's outcomes and overall effectiveness; such information could help FCC identify whether it needs to take steps to address challenges or take other action to further promote wireless network resiliency. Furthermore, FCC does not have any plans to actively communicate information about the framework to public safety officials and industry representatives. A concerted effort by FCC to promote awareness of the framework could help more public safety officials and other industry participants use the framework to prepare for or help mitigate the risks to wireless networks posed by natural disasters and other emergencies.

Recommendations for Executive Action

We are making the following three recommendations to FCC:

The Chairman of FCC should work with industry, to the extent practical, to develop specific and measurable objectives for the Wireless Network Resiliency Cooperative Framework, such as outputs to measure the extent of the framework's use. (Recommendation 1)

The Chairman of FCC should develop a plan to monitor the outputs and outcomes of the Wireless Network Resiliency Cooperative Framework and document the results of its monitoring to evaluate its effectiveness and identify whether changes are needed. (Recommendation 2)

The Chairman of FCC should promote awareness about the elements of and any outcomes from the Wireless Network Resiliency Cooperative Framework among state and local public safety officials and other industry stakeholders, such as through existing outreach mechanisms and government-industry forums. (Recommendation 3)

Agency Comments

We provided a draft of this report to FCC, DHS, and the Department of Commerce for comment. In its comments, reproduced in appendix III, FCC agreed with the recommendations. FCC also provided technical comments, which we incorporated as appropriate. DHS and the Department of Commerce had no comments.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the appropriate congressional committees, the Chairman of FCC, the Secretary of Homeland Security, and the Secretary of Commerce. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-2834 or goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

Sincerely yours,

Mark L. Goldstein
Director, Physical Infrastructure

Appendix I: Objectives, Scope, and Methodology

This report examines federal agency and industry efforts to improve the resiliency of mobile wireless networks in response to natural disasters and other physical incidents since Hurricane Sandy, a natural disaster that caused significant communications outages across several states in late 2012. Specifically, this report examines: (1) trends in mobile wireless outages attributed to physical incidents since 2009 as reported to the Federal Communications Commission (FCC), (2) the actions federal agencies and industry have taken since 2013 to improve wireless network resiliency, and (3) options that federal agencies could take to improve network resiliency and their advantages and disadvantages. This report focuses on the physical risks facing wireless networks; that is, the potential for an unwanted effect from an incident on a network's infrastructure like towers, antennas, and switches. Therefore, we did not examine cyber risks facing wireless networks.

To determine the trends in wireless outages, we analyzed data from FCC's Network Outage Reporting System (NORS) on wireless outages that occurred from 2009 through 2016. We chose this timeframe to cover 4 years of data before and after Hurricane Sandy. Communications providers, including wireless carriers, are required in regulation to submit outage reports in NORS for network service disruptions that reach certain thresholds.[1] Given our focus on wireless outages, we examined reports in NORS for outages (1) that were reported by wireless companies that identified themselves as either a wireless carrier or Voice over Internet Protocol (VoIP) provider[2] and (2) that were cited, as the reason the outage was reportable, a reporting requirement applicable to a wireless carrier or VoIP provider in 47 C.F.R. Part 4.[3]

[1] 47 C.F.R. § 4.

[2] Some wireless carriers have implemented Voice over Long-Term Evolution (also known as VoLTE) networks and thus could report an outage on these wireless networks as a VoIP outage.

[3] We included outages that listed one of the following as the reason for reporting the outage: 1350 DS3 minutes, blocked calls, E911, mobile switching center, other special facilities, VoIP-900,000 user minutes, VoIP-E911, Wireless-900,000 user minutes, and Wireless-E911.

We analyzed NORS data for wireless outages to determine the total number and the causes of wireless outages that occurred from 2009 through 2016. FCC provides carriers a list of 19 main categories from which a carrier selects a root cause, direct cause, and contributing factor(s) for an outage. We examined the root cause and direct cause for each wireless outage reported to FCC. We collapsed several of the FCC categories to create 9 categories for ease of presentation. Table 5 shows the crosswalk between the 19 FCC categories and our 9 collapsed categories.

Table 5: GAO Categories for Wireless Outage Causes for All Outages

GAO combined category	FCC categories
Cable damage/failure	Cable Damage Cable Damage/Malfunction
Equipment failure	Design-Firmware Design-Hardware Design-Software Hardware Failure
Network robustness	Diversity Failure Simplex Condition
Maintenance	Spare Procedural-Other Vendor/Contractor Procedural-Service Provider Procedural-System Vendor Planned Maintenance
External environmental	Environment-External
Internal environmental	Environment-Internal
Other/Insufficient data	Insufficient Data Other/Unknown
Power failure	Power Failure
Traffic/System overload	Traffic/System Overload

Source: GAO. | GAO-18-198

We also analyzed the data to identify the share of all wireless outages attributed to a physical incident—that is, a natural disaster (e.g., flooding, earthquake, wildfire); accident (e.g., backhoe cut); or manmade event (e.g., theft, malicious act). FCC provides carriers a list of categories from which they select a root cause, direct cause, and contributing factor(s) for an outage. Using these FCC categories, we created three new categories for natural disasters, accidents, and manmade events (see table 6). We based these three new categories on the description and categorization of physical risks in FCC and DHS reports, including the *Communications Sector-Specific Plan.*[4]

Table 6: GAO Categories for Wireless Outage Causes for Physical Incidents

GAO category	FCC category	FCC subcategory
Natural disaster	Environment – External	Earthquake Fire Flood Ice/Storm Lightning/Transient Voltage Other Storm-Water/Ice Storm-Wind/Trees
Accident	Cable Damage	Cable Unlocated Digging Error Inaccurate/Incomplete Cable Locate Inadequate/No Notification Other Shallow Cable
	Environment – External	Vehicular Accident Animal
Manmade	Environment – External	Vandalism/Theft

Source: GAO. | GAO-18-198

To understand the distribution of causes across all wireless outages in our time frame, we focused primarily on the root cause for each wireless outage. However, we also examined the root and direct cause reported for each outage to better understand the multiple factors that may have led to an outage and to understand wireless network dependencies (e.g., power, backhaul). Finally, we examined the number of outages, by month and by year, for which a wireless carrier reported a physical event as the root cause, direct cause, or contributing factor to better understand the

[4] U.S. Department of Homeland Security, *Communications Sector-Specific Plan: An Annex to the NIPP 2013* (Washington, D.C.: 2015).

total number of outages related to a physical incident during our time period.[5]

We also analyzed other characteristics of wireless outages such as location, duration, and whether the failure occurred in another company's network. To examine location, we focused on three NORS fields—city, state, and description of location—to identify a city(ies) and state for each outage, and then we determined the latitude and longitude for each outage.[6] We also examined NORS data in conjunction with two other data sets. First, data on events for which FCC activated its Disaster Information Reporting System (DIRS) or "DIRS-lite" to understand any correlation between wireless outages and major physical incidents.[7] Second, data from CTIA's annual wireless survey on the number of wireless subscribers and other measures of wireless networks' size to understand any correlation between wireless outages and the size of the wireless industry.

To assess the reliability of NORS data, we reviewed FCC's data glossary and other FCC documentation on the NORS data system and data elements. We interviewed agency officials responsible for collecting and analyzing NORS data to understand the manual and automated controls used to review carrier-reported outage information and any potential limitations in the data. We also reviewed relevant data elements for missing data, outliers, and errors. We found the data were sufficiently

[5] According to FCC's NORS glossary, the root cause is the underlying reason why the outage occurred or why the outage was reportable and the key problem which, once identified and corrected, will prevent the same or a similar problem from recurring, and the direct cause is the immediate event that results in an outage and is the event, action, or procedure that triggered the outage.

[6] We created and applied an algorithm to identify a city and state in these fields for which we could assign a latitude and longitude; the algorithm enabled us to assign a latitude and longitude for a majority of outages (15,637 of 18,325). When the algorithm could not identify a valid city and state, we manually reviewed information in the outage report to identify a city. When only a county was provided, we identified the county seat as the city for the outage; when an outage was reported as statewide, we identified the state capital as the city for the outage.

[7] DIRS-lite is a scaled back version of DIRS used to determine the status of major wireline and wireless assets, like switches. DIRS is activated only for major disasters while DIRS-lite is activated for smaller-scale disasters. DIRS-lite collects information through email and phone calls. FCC has activated DIRS 14 times and DIRS-lite 6 times since DIRS was created in 2007; 2 of the 14 DIRS activations were later downgraded to DIRS-lite activations. Each activation was for a natural disaster, primarily hurricanes.

reliable for the purpose of describing the number and type of wireless outages reported to FCC that were attributed to a physical incident.

To determine the actions federal agencies have taken since 2013 to improve the resiliency of mobile wireless networks, we reviewed reports and documents from FCC, the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) within the Department of Commerce. Specifically, we reviewed transcripts and papers from hearings and a workshop FCC held in 2013 on communications reliability and continuity. We also analyzed agency orders and comments submitted in FCC's 2013 proceeding on wireless resiliency.[8] In addition, we reviewed communications sector planning reports, such as the 2015 *Communications Sector-Specific Plan* and 2013 *National Infrastructure Protection Plan*,[9] and other DHS communications sector-specific documents, as well as the NIST *Community Resilience Planning Guide for Buildings and Infrastructure Systems* and related documents.[10] We also examined reports from federal advisory committees and partnership councils that cover wireless network resiliency, including reports from the Technological Advisory Council; Communications, Security, Reliability, and Interoperability Council; National Security Telecommunications Advisory Committee; and the Communications Sector Coordinating Council.

To ensure we covered relevant agency actions and to seek any information on the results of these actions, we interviewed officials from DHS's Office of Cybersecurity and Communications within the National Protection and Programs Directorate, including officials from the Stakeholder Engagement and Cyber Infrastructure Resilience division—the sector-specific agency that leads federal efforts to protect and secure the communications critical infrastructure—and National Cybersecurity and Communications Integration Center—the center that continuously monitors incidents that may impact communications. We also interviewed

[8] *In the Matter of Improving the Resiliency of Mobile Wireless Communications Networks*, 28 FCC Rcd 14373 (2013)

[9] *Communications Sector-Specific Plan*, 2015, and DHS, *National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: 2013).

[10] U.S. Department of Commerce, *NIST Special Publication 1190: Community Resilience Planning Guide for Buildings and Infrastructure Systems, Volume I and II* (Washington, D.C.: May 2016).

officials from DHS's Federal Emergency Management Agency and Science and Technology Directorate, FCC, and NIST.

Beyond federal agency officials, we interviewed 24 stakeholders to further understand federal agency and related industry actions to improve wireless network resiliency since 2013 and any results from these actions. Stakeholders included wireless carriers and other owners of wireless network infrastructure, industry associations, consumer groups, and state and local government officials. We selected stakeholders to ensure we covered different perspectives (e.g., industry and consumer groups, associations that represent state and local public safety officials). In particular, we selected industry associations and individual companies to cover both wireless carriers—which operate networks and own some network infrastructure—and communications tower companies—which own and operate towers and sites and then lease space to wireless carriers. We selected wireless carriers to include both nationwide and regional carriers. We selected state agencies to include states directly affected by two events—flooding in Louisiana and Hurricane Matthew—for which industry had implemented elements of the framework at the time we began our review. The views presented in our report are not generalizable to those of all stakeholders. See table 7 for a list of interviewed stakeholders.

Table 7: List of Interviewed Stakeholders

Academic
David Turetsky, professor, University at Albany, State University of New York
Consumer groups
Consumers Union
New America, Resilient Communities Program
Public Knowledge
Industry associations
Alliance for Telecommunications Industry Solutions – Network Reliability Steering Committee
Association of Public-Safety Communications Officials International
Competitive Carriers Association
CTIA
National Emergency Management Association
NTCA - The Rural Broadband Association and Rural Wireless Association
Wireless Infrastructure Association

Infrastructure owners
American Tower
Crown Castle
Partnership council
Communications Sector Coordinating Council
State and local agencies
Georgia Emergency Management and Homeland Security Agency
Louisiana Governor's Office of Homeland Security and Emergency Preparedness
New York City Department of Information Technology and Telecommunications
San Francisco Office of Resiliency and Capital Planning
South Carolina Department of Administration
Wireless carriers
AT&T
GCI
Pioneer
T-Mobile
Verizon

Source: GAO. | GAO-18-198

We reviewed documents describing the Wireless Network Resiliency Cooperative Framework (framework)—a voluntary, industry initiative announced in April 2016. We interviewed CTIA and three of the five wireless carriers that collectively proposed the framework to learn about the impetus for, status of, and any outcomes or lessons learned from use of the framework to date. We also interviewed FCC and DHS about each agency's awareness of and role monitoring industry use of the framework, and we reviewed FCC plans to monitor and share information about the framework. Finally, we asked stakeholders we interviewed, as described above, about their knowledge of and experience with the framework, including any observed outcomes from its use to date. We assessed FCC's efforts to monitor implementation of the framework against *Standards for Internal Control* and FCC's current strategic plan.[11]

To determine what options exist for federal agencies to improve wireless network resiliency, we examined federal agency reports, literature, and other sources. First, we reviewed filings in FCC's 2013 proceeding

[11] GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014) and FCC, *Strategic Plan, 2015-2018* (Washington, D.C.).

examining wireless resiliency, including FCC's orders and comments filed by various parties, for proposed options that federal agencies could take.[12] Second, we conducted a literature review of peer-reviewed articles, government reports, industry publications, and think tank publications from the last 5 years to identify additional options.[13] Third, we examined reports from the aforementioned federal advisory committees on wireless network resiliency, the NIST *Community Resilience Planning Guide for Buildings and Infrastructure Systems*, and the Hurricane Sandy Rebuilding Task Force for recommendations made to federal agencies to enhance wireless network resiliency. From these sources, we identified 11 proposed options that federal agencies could take to improve wireless network resiliency. We eliminated one option—requiring wireless carriers to disclose outage information to the public—as this was the only option that FCC specifically proposed as a new rule in its 2013 proceeding, but ultimately FCC decided not to move forward on this proposal when it decided to not issue a final rule. The identified options were primarily those that FCC could implement, as FCC is the regulatory agency for wireless communications, although DHS or NIST could implement several of the options.

We interviewed a variety of stakeholders, described above, to obtain their views on the advantages, disadvantages, and feasibility of each of the identified options. We used open-ended questions to solicit input on each option rather than provide a list of advantages and disadvantages to stakeholders. We also asked stakeholders if there were additional options for federal agencies to ensure we had a thorough list of options for federal agencies. Based on interviews with stakeholders and federal agencies, we decided not to present two options in our report—establish more formal, ongoing collaboration between wireless carriers and power companies and create a program to facilitate collaborative restoration between wireless carriers and power companies—as federal agencies told us they were already taking actions on these fronts. Therefore, we included federal agencies' actions related to these two options while describing actions taken by federal agencies since 2013. We analyzed information collected through the interviews with stakeholders to identify the most commonly cited advantages and disadvantages, and to

[12] *In the Matter of Improving the Resiliency of Mobile Wireless Communications Networks*, 28 FCC Rcd 14373 (2013).

[13] For the literature review, we searched ProQuest, Scopus, and Science.gov, among other databases.

determine the number of stakeholders that supported or did not support each option. The information collected from stakeholder interviews is not generalizable to all industry stakeholders.

Appendix II: Analysis of FCC Data on Wireless Outages

The figures below provide results from our analysis of Federal Communications Commission (FCC) data on wireless outages from 2009 through 2016. The data is from the Network Outage Reporting System (NORS), the system that wireless carriers and other communications providers use to report information on outages meeting certain threshold as required by regulation. The figures below present information on the number, cause, and duration of all wireless outages reported to FCC for this period.

To describe wireless outages by cause, we use nine categories that collapse several of the FCC categories from which wireless carriers select the root cause, direct cause, and contributing factor(s) when reporting an outage.[1] The following provides a brief description of these nine categories. Appendix I contains information on the scope and methodology for this analysis, including these nine collapsed categories.

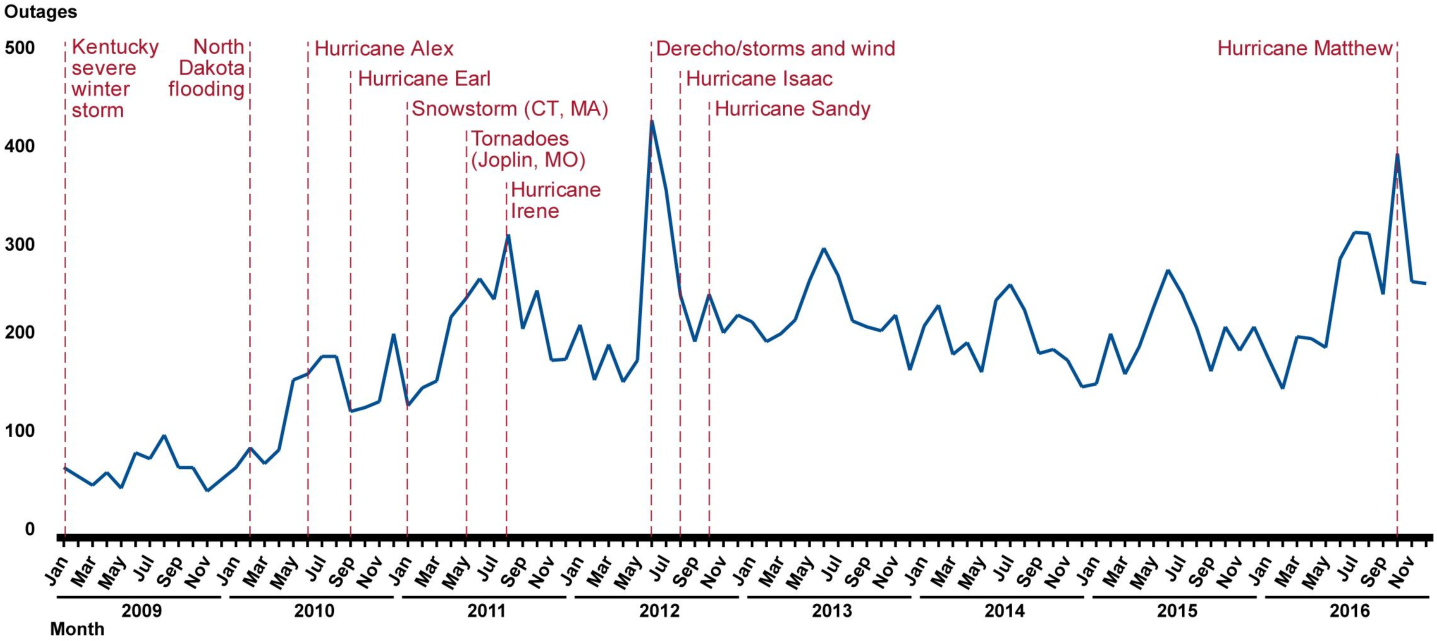
- *Cable damage/failure* includes outages caused by an error locating or digging that resulted in cable damage, by an aerial cable that was damaged or ceased to function, and by loss of transmission in a cable due to aging, among other causes. FCC categories: cable damage, cable damage/malfunction.
- *Equipment failure* contains outages caused by the failure of a hardware component (e.g., circuit pack or card in a processor) or by a problem with the design of firmware, hardware, or software (e.g., failure for firmware to reset or restore after initialization, logical errors in software). FCC categories: design-firmware, design-hardware, design-software, hardware failure.
- *Network robustness* includes outages caused by, for example, a failure to provide or maintain diversity, thus preventing single points of failure. FCC categories: diversity failure, simplex condition.
- *Maintenance* includes outages caused by a needed spare part not being on hand or available, a vendor or contractor lacking updated procedures for its work, a service provider not providing adequate or

[1] FCC, *Network Outage Reporting System, Glossary of Fields in NORS Reports, Version 1* (Washington, D.C., July 25, 2016).

up-to-date training, and scheduled maintenance to upgrade a network component or fix a known problem, among other causes. FCC categories: spare, procedural-other vendor/contractor, procedural-service provider, procedural-system vendor, planned maintenance.

- *External environmental* contains outages caused by earthquakes, wildfires, flooding, and other natural disasters as well as vandalism, theft, vehicle accidents that impair or destroy a component, and animal damage. FCC category: environment (external).
- *Internal environmental* contains outages caused by contamination due to dirt or dust that leads to overheating, by water entering manholes or vaults that destroys or impairs a component, and by other damage related to the condition of buildings and structures housing network equipment. FCC category: environment (internal).
- *Other/Insufficient data* includes outages for which there is not enough information for a failure report or investigation to determine the cause of the failure, service was restored before the cause could be determined, and the cause cannot be determined or proven. FCC categories: insufficient data, other/unknown.
- *Power failure* includes outages due to a commercial power failure (including power failures that extend beyond any backup power capabilities), a generator running out of fuel, a power system that was insufficiently sized for its purpose, and batteries not functioning as designed. FCC category: power failure (commercial and/or backup).
- *Traffic/System overload* contains outages where a network is overloaded or congested because of an unplanned, external event, or because of under-engineering the network due to changing demand or technologies. FCC category: traffic/system overload.

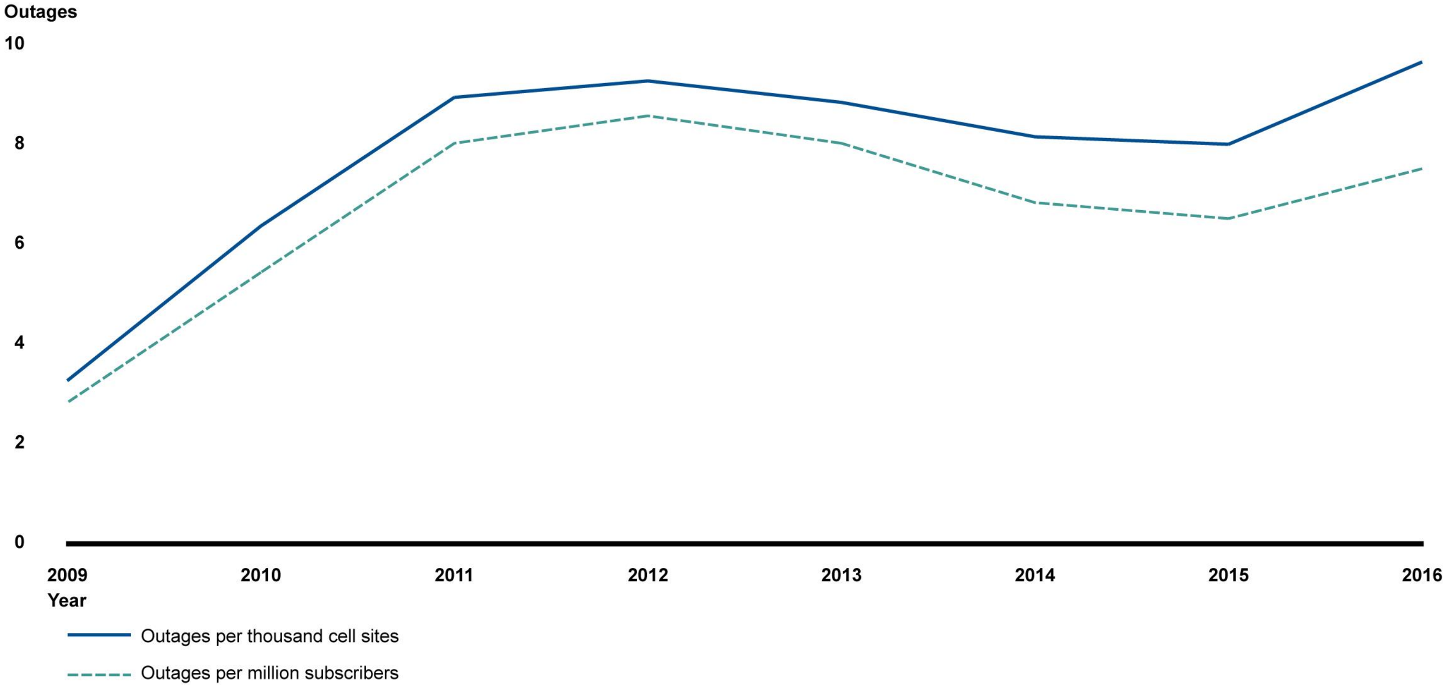
Figure 6: Number of Reported Wireless Outages by Month with Major Natural Disasters, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

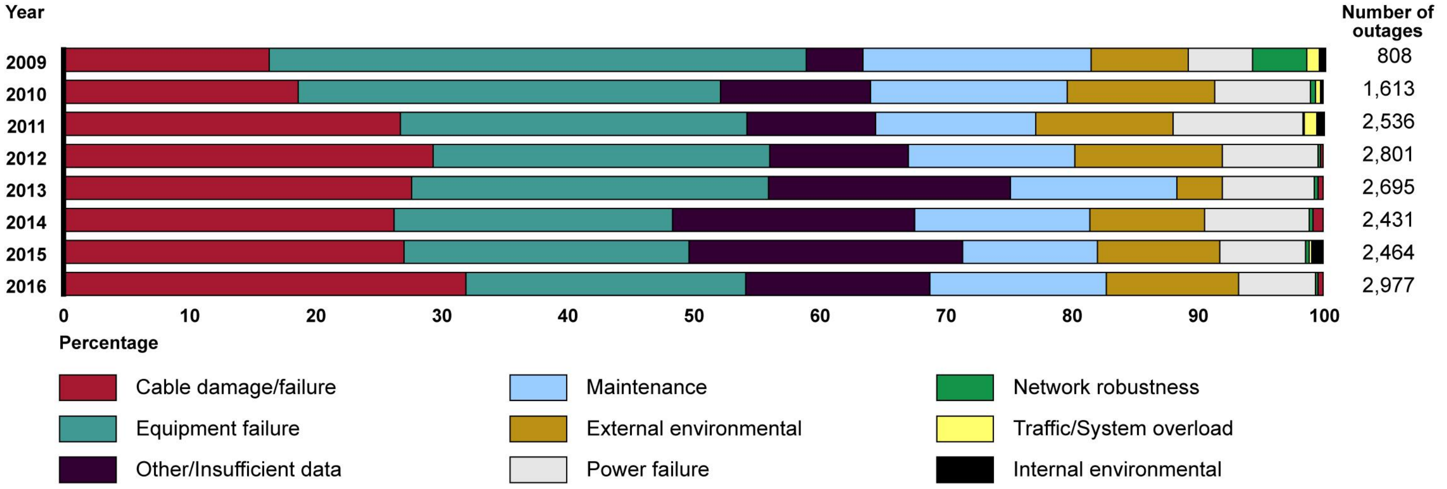
Note: FCC typically suspends NORS reporting requirements in areas where FCC activates DIRS reporting for an emergency event, generally a natural disaster. Therefore, FCC officials said that NORS data can undercount the number of wireless outages due to natural disaster. For a large natural disaster, however, FCC still can receive NORS reports for wireless outages outside the DIRS reporting areas that are due to the natural disaster.

Figure 7: Annual Reported Wireless Outage Rates, 2009–2016



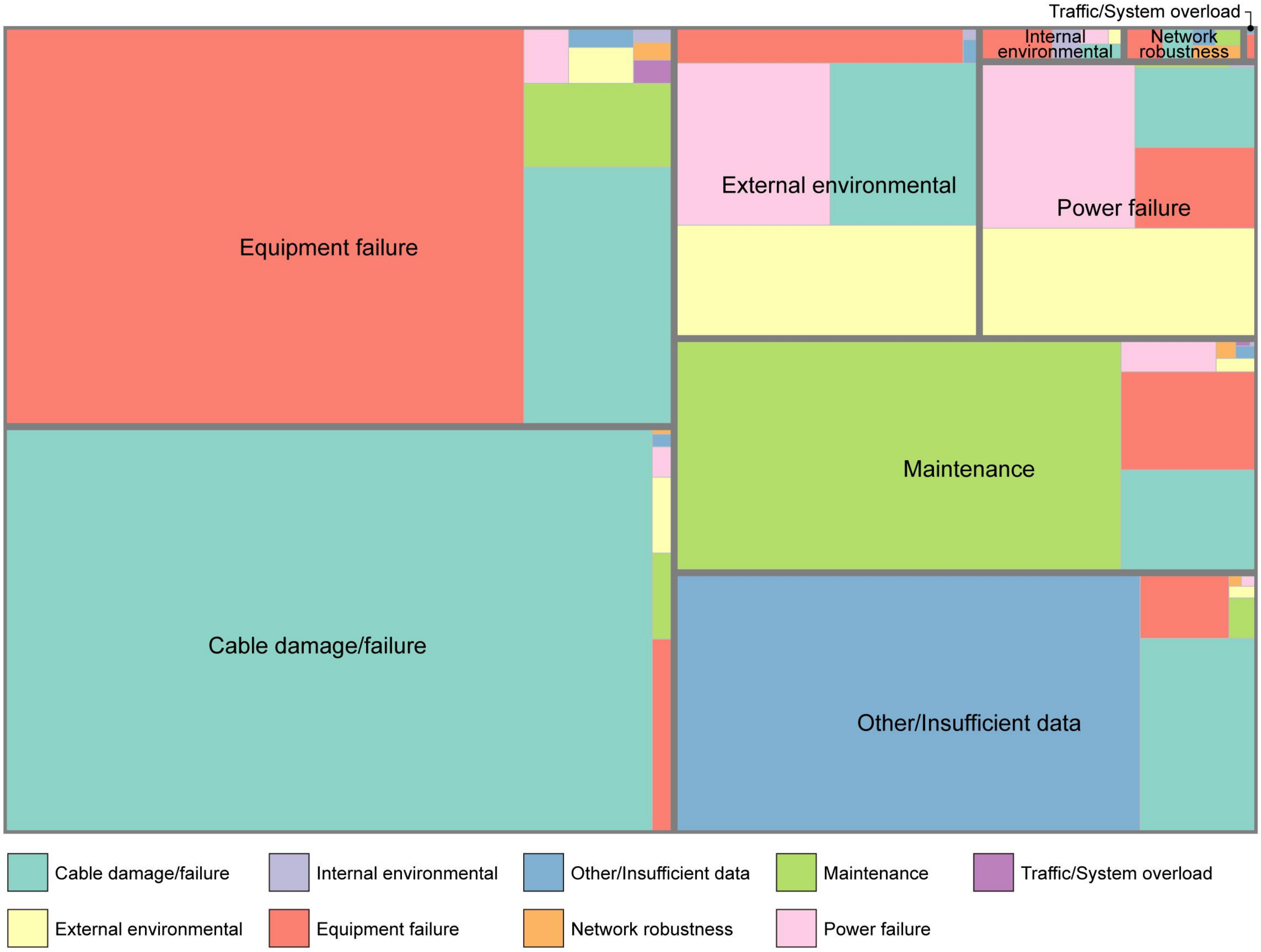
Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

Figure 8: Number and Percentage of Wireless Outages by Reported Root Cause, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

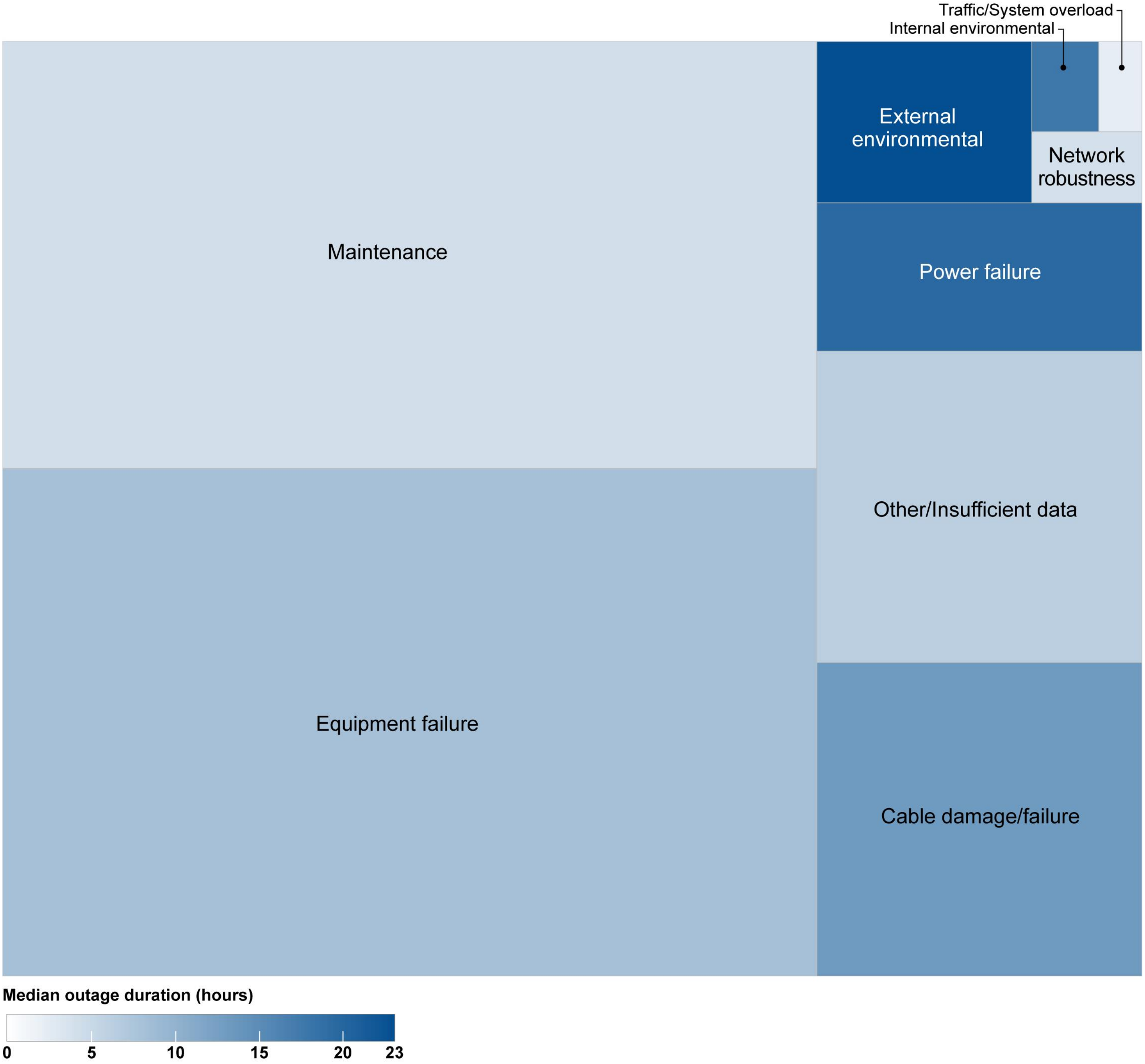
Figure 9: Reported Direct Causes of Wireless Outages, Grouped by Reported Root Cause, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

Note: The large labeled boxes in this graphic represent the root cause reported for an outage, and the smaller boxes within a large box represent the direct cause reported for an outage. The size of a box is determined by the number of outages. Therefore, for root cause, the most commonly reported root causes for wireless outages were equipment failure and cable damage/failure. For outages where equipment failure was the root cause, the most commonly reported direct cause was also equipment failure.

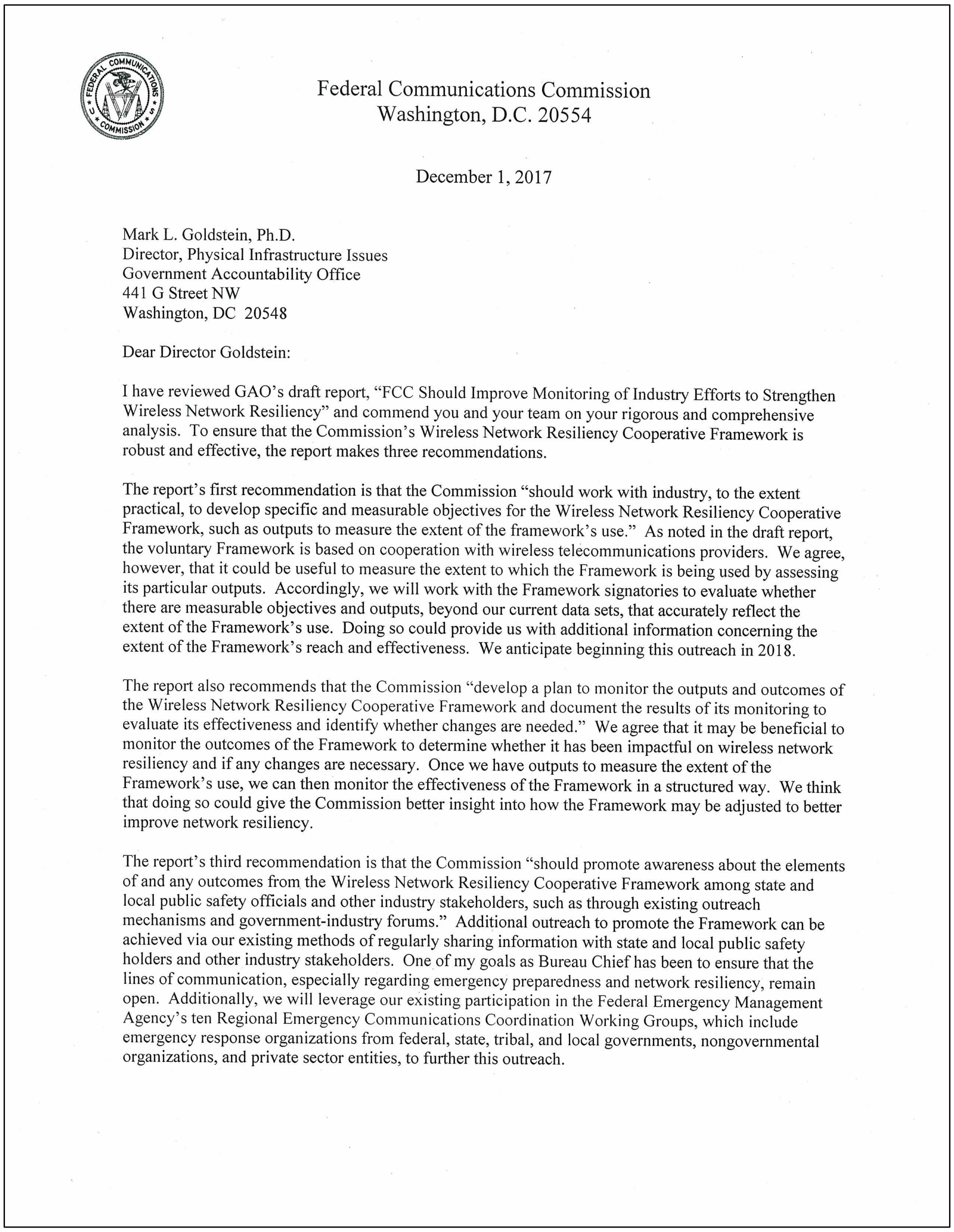
Figure 10: Duration and Number of Users Affected by Reported Wireless Outages, Grouped by Root Cause, 2009–2016



Source: GAO analysis of Federal Communications Commission's Network Outage Reporting System data. | GAO-18-198

Note: The size of each block represents the number of users affected by wireless outages with that root cause, and the shading of the block represents the median duration.

Appendix III: Comments from the Federal Communications Commission



Federal Communications Commission
Washington, D.C. 20554

December 1, 2017

Mark L. Goldstein, Ph.D.
Director, Physical Infrastructure Issues
Government Accountability Office
441 G Street NW
Washington, DC 20548

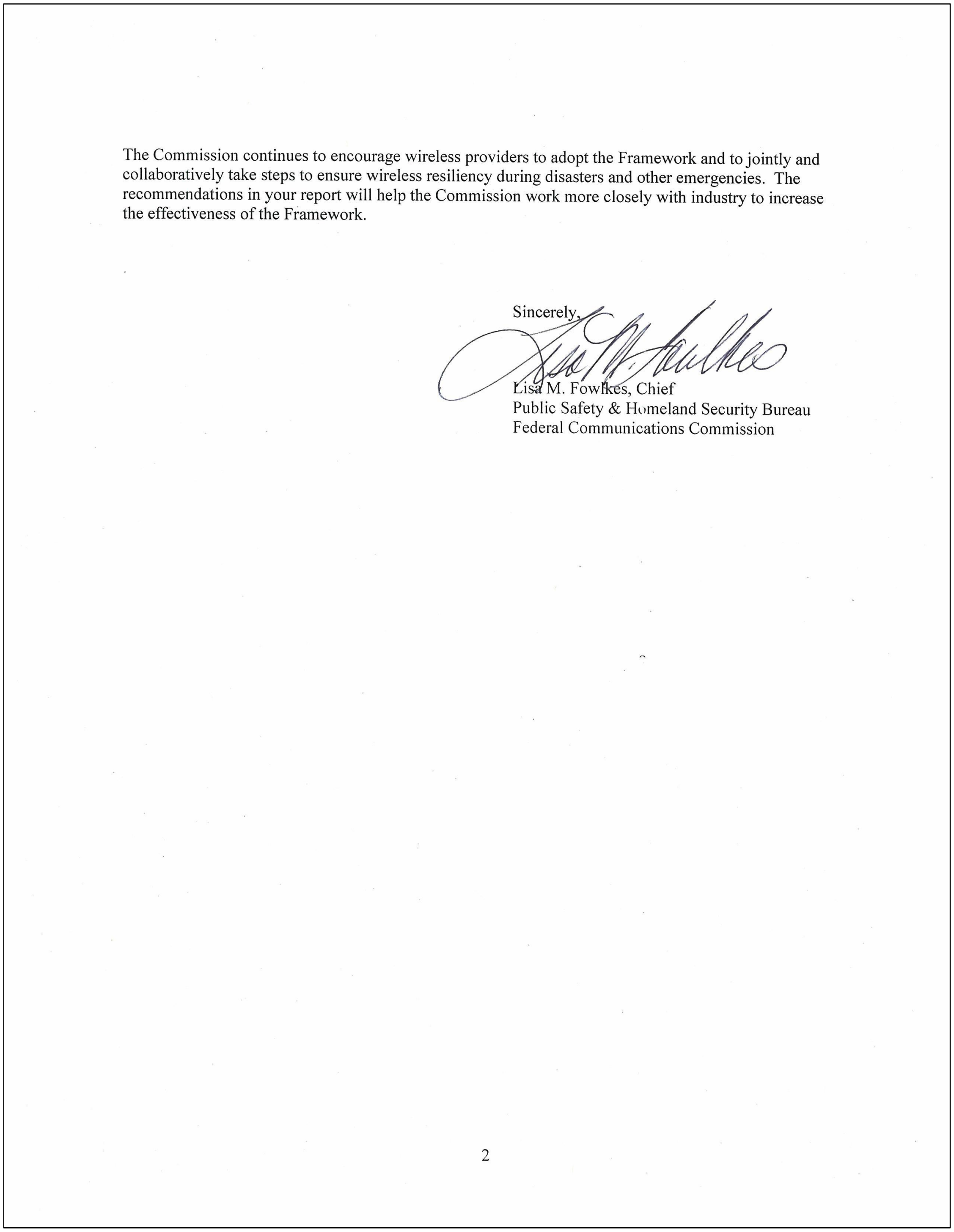
Dear Director Goldstein:

I have reviewed GAO's draft report, "FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency" and commend you and your team on your rigorous and comprehensive analysis. To ensure that the Commission's Wireless Network Resiliency Cooperative Framework is robust and effective, the report makes three recommendations.

The report's first recommendation is that the Commission "should work with industry, to the extent practical, to develop specific and measurable objectives for the Wireless Network Resiliency Cooperative Framework, such as outputs to measure the extent of the framework's use." As noted in the draft report, the voluntary Framework is based on cooperation with wireless telecommunications providers. We agree, however, that it could be useful to measure the extent to which the Framework is being used by assessing its particular outputs. Accordingly, we will work with the Framework signatories to evaluate whether there are measurable objectives and outputs, beyond our current data sets, that accurately reflect the extent of the Framework's use. Doing so could provide us with additional information concerning the extent of the Framework's reach and effectiveness. We anticipate beginning this outreach in 2018.

The report also recommends that the Commission "develop a plan to monitor the outputs and outcomes of the Wireless Network Resiliency Cooperative Framework and document the results of its monitoring to evaluate its effectiveness and identify whether changes are needed." We agree that it may be beneficial to monitor the outcomes of the Framework to determine whether it has been impactful on wireless network resiliency and if any changes are necessary. Once we have outputs to measure the extent of the Framework's use, we can then monitor the effectiveness of the Framework in a structured way. We think that doing so could give the Commission better insight into how the Framework may be adjusted to better improve network resiliency.

The report's third recommendation is that the Commission "should promote awareness about the elements of and any outcomes from the Wireless Network Resiliency Cooperative Framework among state and local public safety officials and other industry stakeholders, such as through existing outreach mechanisms and government-industry forums." Additional outreach to promote the Framework can be achieved via our existing methods of regularly sharing information with state and local public safety holders and other industry stakeholders. One of my goals as Bureau Chief has been to ensure that the lines of communication, especially regarding emergency preparedness and network resiliency, remain open. Additionally, we will leverage our existing participation in the Federal Emergency Management Agency's ten Regional Emergency Communications Coordination Working Groups, which include emergency response organizations from federal, state, tribal, and local governments, nongovernmental organizations, and private sector entities, to further this outreach.



The Commission continues to encourage wireless providers to adopt the Framework and to jointly and collaboratively take steps to ensure wireless resiliency during disasters and other emergencies. The recommendations in your report will help the Commission work more closely with industry to increase the effectiveness of the Framework.

Sincerely,

Lisa M. Fowlkes, Chief
Public Safety & Homeland Security Bureau
Federal Communications Commission

2

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Mark L. Goldstein, (202) 512-2834 or goldsteinm@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Sally Moino (Assistant Director); Joanie Lofgren (Analyst in Charge); Enyinnaya David Aja; Stephen Brown; David Hooper; Richard Hung; Joshua Ormond; Amy Rosewarne; Andrew Stavisky; and Timothy Young made key contributions to this report. Jon Ludwigson, John Mortin, Mark Pross, Pam Snedden, James R Sweetman, Jr., and Joe Thompson also made contributions to this report.

Appendix V: Accessible Data

Data Tables

Data Table for Figure 2: Number of Reported Wireless Outages and Wireless Outages with a Physical Incident as the Root Cause, 2009–2016

Year	Accident	Natural disaster	Manmade	Other
2009	131	57	1	619
2010	287	171	7	1148
2011	650	257	10	1619
2012	756	308	9	1728
2013	677	83	8	1927
2014	534	182	9	1706
2015	592	178	16	1678
2016	813	263	3	1898

Data Table for Figure 3: Number of Reported Wireless Outages for Which a Physical Incident Was Cited as a Cause or Contributing Factor by Month, 2009–2016

Monthly date	Natural disaster	Accident	Manmade
Jan-09	13	21	0
Feb-09	4	11	0
Mar-09	4	9	0
Apr-09	2	14	1
May-09	4	5	0
Jun-09	7	15	0
Jul-09	5	14	0
Aug-09	5	22	0
Sep-09	4	9	0
Oct-09	5	5	0
Nov-09	3	4	0
Dec-09	16	5	0
Jan-10	8	6	1
Feb-10	42	6	0
Mar-10	18	10	0
Apr-10	5	16	0
May-10	18	30	1

Monthly date	Natural disaster	Accident	Manmade
Jun-10	11	29	1
Jul-10	25	34	1
Aug-10	29	40	0
Sep-10	8	28	1
Oct-10	3	28	0
Nov-10	5	32	2
Dec-10	18	40	1
Jan-11	18	30	0
Feb-11	15	32	0
Mar-11	10	36	1
Apr-11	35	58	0
May-11	25	74	0
Jun-11	26	59	0
Jul-11	17	68	0
Aug-11	50	81	3
Sep-11	13	64	0
Oct-11	55	73	1
Nov-11	10	52	3
Dec-11	9	56	2
Jan-12	8	68	1
Feb-12	7	46	0
Mar-12	8	67	0
Apr-12	11	64	1
May-12	6	56	0
Jun-12	177	84	1
Jul-12	66	112	0
Aug-12	11	77	1
Sep-12	7	60	2
Oct-12	7	64	0
Nov-12	4	50	2
Dec-12	18	35	2
Jan-13	11	45	3
Feb-13	5	33	0
Mar-13	7	49	0
Apr-13	8	49	1
May-13	7	57	0
Jun-13	15	84	0

Monthly date	Natural disaster	Accident	Manmade
Jul-13	6	77	0
Aug-13	1	51	2
Sep-13	11	69	1
Oct-13	8	59	0
Nov-13	10	61	1
Dec-13	10	50	0
Jan-14	7	51	0
Feb-14	50	65	0
Mar-14	15	47	0
Apr-14	15	51	0
May-14	8	37	0
Jun-14	15	63	1
Jul-14	26	57	1
Aug-14	15	48	0
Sep-14	7	40	0
Oct-14	7	40	1
Nov-14	11	25	2
Dec-14	13	21	4
Jan-15	10	32	2
Feb-15	29	37	2
Mar-15	9	16	5
Apr-15	12	32	2
May-15	17	54	0
Jun-15	32	59	0
Jul-15	17	71	0
Aug-15	21	61	0
Sep-15	7	56	1
Oct-15	12	74	3
Nov-15	2	63	1
Dec-15	19	47	0
Jan-16	14	39	1
Feb-16	11	40	0
Mar-16	11	59	0
Apr-16	16	42	0
May-16	10	52	1
Jun-16	13	68	1
Jul-16	20	96	0

Monthly date	Natural disaster	Accident	Manmade
Aug-16	24	100	0
Sep-16	9	88	0
Oct-16	115	89	0
Nov-16	15	72	1
Dec-16	18	74	0

Data Table for Figure 4: Median Duration of Reported Wireless Outages due to a Physical Incident, in Hours, by Root Cause, 2009–2016

Year	Accident	Manmade	Natural disaster
2009	7.63	19.32	23.53
2010	11.57	9.38	22.6
2011	15.74	15.73	19.05
2012	12.88	18.07	35.74
2013	12.82	13.43	27.75
2014	12.16	9.87	21.52
2015	13.29	11.46	21.25
2016	13.33	11.37	30.13

Data Table for Figure 5: Number of Wireless Outages with a Physical Incident as the Root Cause, by State and Region, 2009–2016

Region/State	2009	2010	2011	2012	2013	2014	2015	2016
East North Central								
Illinois	12	16	27	31	44	30	31	45
Indiana	2	3	14	25	28	25	27	24
Michigan	2	4	22	26	18	31	17	24
Ohio	9	14	32	78	36	22	31	22
Wisconsin	1	2	5	6	10	8	11	15
East South Central								
Alabama	1	2	11	19	29	26	27	20
Kentucky	3	0	3	10	4	2	4	4
Mississippi	1	0	0	2	2	2	0	1
Tennessee	4	12	23	19	21	35	30	34
Mid-Atlantic								
Delaware	0	1	3	3	4	3	6	2
New Jersey	2	27	37	28	26	16	11	25
New York	8	71	117	115	60	51	62	102
Pennsylvania	5	34	61	68	51	44	34	33

Region/State	2009	2010	2011	2012	2013	2014	2015	2016
Mountain								
Arizona	2	5	3	5	2	3	11	6
Colorado	1	8	18	9	21	18	29	16
Idaho	0	3	0	1	3	4	1	2
Montana	3	1	9	11	2	7	2	7
Nevada	3	1	2	6	5	4	2	2
New Mexico	2	2	3	5	7	3	6	4
Utah	4	3	6	4	8	1	3	5
Wyoming	0	1	1	0	0	0	0	0
New England								
Connecticut	0	2	6	3	1	1	2	2
Maine	0	1	4	0	0	0	0	1
Massachusetts	0	13	45	12	6	7	9	15
New Hampshire	1	1	3	0	7	8	0	1
Rhode Island	0	2	8	1	0	0	0	0
Vermont	0	1	1	1	0	1	0	0
Pacific								
Alaska	0	0	0	0	0	2	2	0
California	17	25	47	44	49	59	59	67
Hawaii	1	3	5	2	6	2	8	1
Oregon	4	4	10	7	4	8	6	10
Washington	3	5	8	13	10	22	21	13
South Atlantic								
District of Columbia	1	18	4	5	4	3	3	4
Florida	10	22	31	32	14	20	25	49
Georgia	7	10	23	31	24	42	41	72
Maryland	0	14	34	111	15	8	13	16
North Carolina	11	14	27	18	23	31	38	80
South Carolina	2	16	17	27	26	42	47	120
Virginia	13	21	62	104	26	20	31	43
West Virginia	5	9	16	40	7	3	0	5
West North Central								
Iowa	0	1	1	3	5	5	2	5
Kansas	2	2	7	15	7	8	8	5
Minnesota	1	3	18	15	13	19	9	26
Missouri	4	2	16	17	14	13	6	22
Nebraska	0	3	3	1	3	5	11	9

Region/State	2009	2010	2011	2012	2013	2014	2015	2016
North Dakota	0	1	1	4	2	2	1	5
South Dakota	0	2	3	0	2	1	0	3
West South Central								
Arkansas	6	6	13	18	14	10	19	11
Louisiana	3	2	9	12	19	12	11	18
Oklahoma	4	1	8	9	9	1	6	10
Texas	21	31	59	49	71	35	54	58

Data Table for Figure 6: Number of Reported Wireless Outages by Month with Major Natural Disasters, 2009–2016

Month	Outages
Jan 2009	70
Feb 2009	61
Mar 2009	52
Apr 2009	65
May 2009	49
Jun 2009	85
Jul 2009	79
Aug 2009	103
Sep 2009	70
Oct 2009	70
Nov 2009	46
Dec 2009	58
Jan 2010	70
Feb 2010	90
Mar 2010	74
Apr 2010	88
May 2010	159
Jun 2010	165
Jul 2010	183
Aug 2010	183
Sep 2010	127
Oct 2010	131
Nov 2010	137
Dec 2010	206
Jan 2011	133
Feb 2011	151

Month	Outages
Mar 2011	158
Apr 2011	223
May 2011	241
Jun 2011	262
Jul 2011	241
Aug 2011	307
Sep 2011	211
Oct 2011	250
Nov 2011	179
Dec 2011	180
Jan 2012	215
Feb 2012	159
Mar 2012	195
Apr 2012	157
May 2012	179
Jun 2012	423
Jul 2012	352
Aug 2012	245
Sep 2012	198
Oct 2012	246
Nov 2012	207
Dec 2012	225
Jan 2013	218
Feb 2013	198
Mar 2013	206
Apr 2013	220
May 2013	260
Jun 2013	293
Jul 2013	265
Aug 2013	219
Sep 2013	213
Oct 2013	209
Nov 2013	225
Dec 2013	169
Jan 2014	214
Feb 2014	235
Mar 2014	185

Month	Outages
Apr 2014	197
May 2014	167
Jun 2014	240
Jul 2014	256
Aug 2014	230
Sep 2014	186
Oct 2014	190
Nov 2014	179
Dec 2014	152
Jan 2015	155
Feb 2015	206
Mar 2015	165
Apr 2015	193
May 2015	233
Jun 2015	271
Jul 2015	246
Aug 2015	212
Sep 2015	168
Oct 2015	213
Nov 2015	189
Dec 2015	213
Jan 2016	181
Feb 2016	150
Mar 2016	203
Apr 2016	201
May 2016	192
Jun 2016	282
Jul 2016	309
Aug 2016	308
Sep 2016	246
Oct 2016	389
Nov 2016	259
Dec 2016	257

Data Table for Figure 7: Annual Reported Wireless Outage Rates, 2009–2016

Year	Outages per thousand cell sites	Outages per million subscribers
2009	3.27	2.83
2010	6.37	5.44
2011	8.95	8.03
2012	9.28	8.58
2013	8.85	8.03
2014	8.16	6.84
2015	8.01	6.52
2016	9.66	7.52

Data Table for Figure 8: Number and Percentage of Wireless Outages by Reported Root Cause, 2009–2016

Year	Cable damage/failure	Equipment failure	Other/Insufficient data	Maintenance	External environmental	Power failure	Network robustness	Traffic/System overload	Internal environmental
2009	16.3	42.6	4.5	18.1	7.7	5.1	4.3	1	0.5
2010	18.6	33.5	11.9	15.6	11.7	7.6	0.4	0.4	0.2
2011	26.7	27.5	10.2	12.7	10.9	10.3	0.1	1	0.6
2012	29.3	26.7	11	13.2	11.7	7.6	0.2	0	0.2
2013	27.6	28.3	19.2	13.2	3.6	7.3	0.3	0	0.4
2014	26.2	22.1	19.2	13.9	9.1	8.3	0.3	0	0.8
2015	27	22.6	21.7	10.7	9.7	6.8	0.3	0.2	0.9
2016	31.9	22.2	14.6	14	10.5	6.1	0.2	0	0.4

Data Table for Figure 9: Reported Direct Causes of Wireless Outages, Grouped by Reported Root Cause, 2009–2016

Root cause	Direct cause	Number of outages
Cable damage/failure	Cable damage/failure	4767
Cable damage/failure	External environment	30
Cable damage/failure	Equipment failure	77
Cable damage/failure	Other/Insufficient data	5
Cable damage/failure	Network robustness	3
Cable damage/failure	Maintenance	34
Cable damage/failure	Power failure	12
External environment	Cable damage/failure	437
External environment	External environment	624
External environment	Internal environment	4
External environment	Equipment failure	193

Root cause	Direct cause	Number of outages
External environment	Other/Insufficient data	7
External environment	Power failure	456
Internal environment	Cable damage/failure	14
Internal environment	External environment	5
Internal environment	Internal environment	18
Internal environment	Equipment failure	47
Internal environment	Power failure	9
Equipment failure	Cable damage/failure	704
Equipment failure	External environment	42
Equipment failure	Internal environment	12
Equipment failure	Equipment failure	3762
Equipment failure	Other/Insufficient data	25
Equipment failure	Network robustness	13
Equipment failure	Maintenance	227
Equipment failure	Power failure	46
Equipment failure	Traffic/System Overload	17
Other/Insufficient data	Cable damage/failure	415
Other/Insufficient data	External environment	6
Other/Insufficient data	Equipment failure	105
Other/Insufficient data	Other/Insufficient data	2194
Other/Insufficient data	Network robustness	3
Other/Insufficient data	Maintenance	21
Other/Insufficient data	Power failure	3
Other/Insufficient data	Traffic/System overload	1
Network robustness	Cable damage/failure	19
Network robustness	External environment	1
Network robustness	Internal environment	1
Network robustness	Equipment failure	25
Network robustness	Other/Insufficient data	8
Network robustness	Network robustness	15
Network robustness	Maintenance	8
Maintenance	Cable damage/failure	254
Maintenance	External environment	10
Maintenance	Internal environment	1
Maintenance	Equipment failure	242
Maintenance	Other/Insufficient data	5
Maintenance	Network robustness	7

Root cause	Direct cause	Number of outages
Maintenance	Maintenance	1889
Maintenance	Power failure	57
Maintenance	Traffic/System overload	2
Power failure	Cable damage/failure	177
Power failure	External environment	554
Power failure	Internal environment	3
Power failure	Equipment failure	179
Power failure	Maintenance	10
Power failure	Power failure	467
Traffic/System overload	Equipment failure	7
Traffic/System overload	Other/Insufficient data	2

Data Table for Figure 10: Duration and Number of Users Affected by Reported Wireless Outages, Grouped by Root Cause, 2009–2016

Root cause	Users affected	Median duration (hours)
Cable damage/failure	89351802	13.12
External environment	30380440	23.05
Internal environment	5299612	17.79
Equipment failure	362048121	8.19
Other/Insufficient data	88611412	6.28
Network robustness	6864980	4.00
Maintenance	304533580	4.25
Power failure	42302246	19.66
Traffic/System overload	3430125	2.23

Agency Comment Letter

Text of Appendix III: Comments from the Federal Communications Commission

Page 1

December 1, 2017

Mark L. Goldstein, Ph.D.

Director, Physical Infrastructure Issues Government Accountability Office 441 G Street NW

Washington, DC 20548 Dear Director Goldstein:

I have reviewed GAO's draft repo 1t , "FCC Should Improve Monitoring of Industry Efforts to Strengthen Wireless Network Resiliency" and commend you and your team on your rigorous and comprehensive analysis. To ensure that the Commission ' s Wireless Network Resiliency Cooperative Framework is robust and effective, the report makes three recommendations.

The report's first recommendation is that the Commission "should work with industry, to the extent practical, to develop specific and measurable objectives for the Wireless Network Resiliency Cooperative Framework, such as outputs to measure the extent of the framework's use." As noted in the draft report, the voluntary Framework is based on cooperation with wireless telecommunications providers. We agree, however, that it could be useful to measure the extent to which the Framework is being used by assessing its particular outputs. According ly, we will work with the Framework signatories to evaluate whether there are measurable objectives and outputs, beyond our current data sets, that accurately reflect the extent of the Framework's use. Doing so could provide us with additional information concerning the extent of the Framework's reach and effectiveness. We anticipate beginning this outreach in 2018.

The report also recommends that the Commission " develop a plan to monitor the outputs and outcomes of the Wireless Network Resiliency Cooperative Framework and document the results of its monitoring to evaluate its effectiveness and identify whether changes are needed. " We agree that it may be beneficial to monitor the outcomes of the Framework to determine whether it has been impactful on wireless network resiliency and if any changes are necessary. Once we have outputs to measure the extent of the Framework ' s use, we can then monitor the effectiveness of the Framework in a structured way. We think that doing so could give the Commission better insight into how the Framework may be adjusted to better improve network resiliency .

The report's third recommendation is that the Commission "should promote awareness about the elements of and any outcomes from. the Wireless Network Resiliency Cooperative Framework among state and local public safety officials and other industry stakeholders, such as through existing outreach mechanisms and government-industry forums."

Additional outreach to promote the Framework can be achieved via our existing methods of regularly sharing information with state and local public safety holders and other industry stakeholders. One of my goals as Bureau Chief has been to ensure that the lines of communication, especially regarding emergency preparedness and network resiliency, remain open. Additionally, we will leverage our existing participation in the Federal Emergency Management Agency ' s ten Regional Emergency Communications Coordination Working Groups , which include emergency response organizations from federal, state, tribal, and local governments, nongovernmental organizations, and private sector entities, to further this outreach.

Page 2

The Commission continues to encourage wireless providers to adopt the Framework and to jointly and collaboratively take steps to ensure wireless resiliency during disasters and other emergencies. The recommendations in your report will help the Commission work more closely with industry to increase the effectiveness of the Framework.

Lisa Fowlkes,

ChiefPublic Safety & Homeland Security Bureau Federal Communications Commission

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548