United States Government Accountability Office

Report to Congressional Requesters

December 2015

# INTERNET PROTOCOL TRANSITION

# FCC Should Strengthen Its Data Collection Efforts to Assess the Transition's Effects

GAO-16-167

December 2015

# INTERNET PROTOCOL TRANSITION

## FCC Should Strengthen Its Data Collection Efforts to Assess the Transition's Effects

GAO Highlights

Highlights of GAO-16-167, a report to congressional requesters

## Why GAO Did This Study

The communications sector is essential to the nation's economy and government operations and for the delivery of public safety services, especially during emergencies. As the sector transitions from legacy networks to IP-based networks, consumer and public safety groups and others have raised concerns about how the communications networks will function during times of crisis.

GAO was asked to examine the reliability of the nation's communications network in an IP environment during times of crisis. GAO examined (1) the potential challenges affecting IP networks in times of crisis and how the challenges may affect end users, and (2) the actions FCC, DHS, and other stakeholders have taken to ensure the reliability of IP communications. GAO reviewed FCC and DHS documents as well as FCC proceedings and comments filed with FCC on the IP transition and emergency communications. GAO assessed FCC's efforts to collect data on the effect of the IP transition. GAO interviewed officials from FCC and DHS, and representatives from the three largest telecommunications carriers, industry associations, and public interest and consumer advocacy groups.

## What GAO Recommends

FCC should strengthen its data collection efforts to assess the IP transition's effects. FCC did not agree or disagree with the recommendation and stated it has a strategy in place to oversee the IP transition. However, GAO continues to believe FCC should strengthen its data collection efforts.

View GAO-16-167. For more information, contact Mark Goldstein at (202) 512-2834 or GoldsteinM@gao.gov.

## What GAO Found

As the nation's telecommunications systems transition from legacy telephone networks to Internet Protocol (IP)-based networks, telecommunications carriers can face challenges during times of crisis that affect end users' ability to call 911 and receive emergency communications. These challenges include (1) preserving consumer service and (2) supporting existing emergency communications services and equipment. For example, during power outages, consumers with service provided over IP networks and without backup power can lose service. The Federal Communications Commission (FCC) is working to address this issue by adopting rules that will require carriers to provide information to consumers on backup power sources, among other things. Another challenge is that IP networks may not support existing telecommunications "priority" services, which allow key government and public-safety officials to communicate during times of crisis.

FCC, the Department of Homeland Security (DHS), and telecommunications carriers have taken various steps to ensure the reliability of IP communications, for example:

- FCC proposed criteria—such as support for 911 services, network security, and access for people with disabilities—to evaluate carriers' replacement of legacy services when carriers seek to discontinue existing service.
- DHS coordinated the development of the *Communications Sector Specific Plan* to help protect the nation's communications infrastructure.
- Carriers told GAO they build resiliency and reliability into their IP networks as part of business operations and emergency planning.

FCC is also collecting data on the IP transition, but FCC could do more to ensure it has the information it needs to make data-driven decisions about the transition. FCC has emphasized that one of its statutory responsibilities is to ensure that its core values, including public safety capabilities and consumer protection, endure as the nation transitions to modernized networks. FCC stated that fulfilling this responsibility requires learning more about how the transition affects consumers. FCC plans on collecting data on the IP transition primarily through voluntary experiments proposed and run by telecommunications carriers. However, it is unclear if FCC will be able to make data-driven decisions about the IP transition because of the limited number and scale of the proposed experiments. In particular, there are only three proposed experiments that cover a very limited number of consumers; none of the experiments covers consumer services in high-density urban areas or includes critical national-security or public-safety locations. FCC also sought comment on how to supplement its data-gathering process; however, soliciting comments may not necessarily result in a change in FCC's existing policies. GAO found FCC lacks a detailed strategy that outlines how it will address its remaining information needs. Developing a strategy for collecting information about how the IP transition affects public safety and consumers would help FCC make data-driven decisions and address areas of uncertainty as it oversees the IP transition.

# Contents

## Abbreviations

| | |
|---|---|
| APCO | Association of Public Safety Communications Officials International |
| ATIS | Alliance for Telecommunications Industry Solutions |
| Communications Act | Communications Act of 1934, as amended |
| CSRIC | Communications Security, Reliability, and Interoperability Council |
| DHS | Department of Homeland Security |
| DIRS | Disaster Information Reporting System |
| FCC | Federal Communications Commission |
| GETS | Government Emergency Telecommunications Service |
| IP | Internet Protocol |
| NORS | Network Outage Reporting System |
| TDM | time-division multiplexed |
| VoIP | Voice over Internet Protocol |

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

December 16, 2015

The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

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

The communications sector is essential to the nation's economy, public safety, and government operations. As part of the nation's critical infrastructure, 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.[1] Furthermore, communications services play an essential role in the delivery of public safety services, especially during emergencies. The communications sector is transitioning from legacy networks to an all-Internet Protocol (IP) environment, leading consumer and public safety groups, among others, to question how reliably the nation's communications networks will function during times of crisis, such as natural and man-made disasters. While the private sector owns and operates the nation's communications networks and is primarily in charge of managing and protecting these assets, federal law and policy establish regulatory and support roles for the federal government related to communications networks. In particular, the Federal Communications Commission (FCC) and Department of Homeland Security (DHS) have roles in enhancing the cyber and physical security of the communications infrastructure that is essential to national security and public health and safety.

[1]According to Executive Order 13636, critical infrastructure consists of the assets and systems, whether physical or virtual, 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, or any combination thereof. 78 Fed. Reg. 11739 (Feb. 19, 2013).

The communications sector's infrastructure is in the midst of a significant change, which FCC refers to as a series of technology transitions from legacy networks built for one specific purpose (e.g., telephone calls) to IP-based networks built for a variety of purposes (e.g., broadband, video, data, voice, etc.).[2] According to FCC, modernizing communications networks through this and other means can dramatically reduce network costs and broaden access to new technologies, allowing telecommunications carriers to serve customers with increased efficiencies that can lead to improved and innovative product offerings and lower prices. The IP transition, however, is a gradual shift; thus, it will take many years to complete and has no specific end date. In 2014, FCC established a framework for telecommunications carriers to conduct voluntary "service-based" experiments, whereby carriers could substitute new communications technologies, such as fiber and cable for the services that they currently provide to customers over legacy copper lines.[3] According to FCC, these voluntary service-based experiments will examine the effects of replacing existing customer services with IP-based alternatives.

You asked us to review issues related to the reliability of the nation's communications network in an IP environment during times of crisis, which could include weather events (e.g., hurricanes or flooding); man-made disasters (e.g., vandalism or terrorist attacks); and unintentional man-made outages (e.g., a backhoe cutting a communication line). This report examines (1) the potential challenges affecting IP networks in times of crisis and how the challenges affect end users, and (2) the actions FCC, DHS, and other stakeholders have taken to ensure the reliability of IP communications during times of crisis.

To address these objectives, we reviewed relevant FCC and DHS documents including orders, notices of proposed rulemakings, reports, and risk assessments, as well as relevant statutes and regulations. We reviewed comments filed with FCC regarding the IP transition and emergency communications. To ensure we reviewed a broad range of comments, we selected comments by stakeholders that represented a variety of interests, including public interest groups, industry and trade associations, and state and local authorities. To identify information on

[2]In this report, we refer to this change as the IP transition.

[3]79 Fed. Reg. 11327 (Feb. 28, 2014).

the proposed IP transition service-based experiments, we reviewed three experiment proposals submitted by telecommunications carriers, stakeholder comments to FCC on these proposals, and other documents related to the service-based experiments.[4] We assessed FCC's efforts to collect data on the effect of the IP transition against criteria established in the federal Standards for Internal Control.[5] We reviewed relevant DHS documents including the 2013 *National Infrastructure Protection Plan*, the 2010 *Communications Sector Specific Plan*, and the *2012 Risk Assessment Report for Communications*. We interviewed state and local officials and other stakeholders in six states—New York, New Jersey, Arizona, California, Florida, and Alabama—to obtain additional information on the challenges facing IP networks and how these challenges affect end users, and to obtain information on state efforts to ensure reliability. We selected these locations because they represent a mix of communities that have experienced a major communications outage since 2012 or that contain an area with a proposed IP transition experiment. These communities also contain a mix of rural, suburban, and urban communities, and demographics including economic differences and average age of residents. We also interviewed officials from FCC, DHS, and representatives from selected stakeholder groups including public-interest and consumer-advocacy groups, industry associations, the three largest telecommunications companies, and other stakeholders. We identified stakeholders to interview based on our review of comments filed in FCC's Technology Transitions proceeding, as well as based on recommendations from other organizations we interviewed. More details about our scope and methodology can be found in appendix I.

We conducted this performance audit from December 2014 to December 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to

[4]At the time of our review, FCC had received three service-based experiment proposals, two of which were submitted by AT&T and one by CenturyLink.

[5]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999). The most recent version of these standards was issued in September 2014 and becomes effective October 1, 2015. GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014). We did not use the new standards to assess FCC's efforts to collect data on the effect of the IP transition because the new standards were not in effect at the time of our review.

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

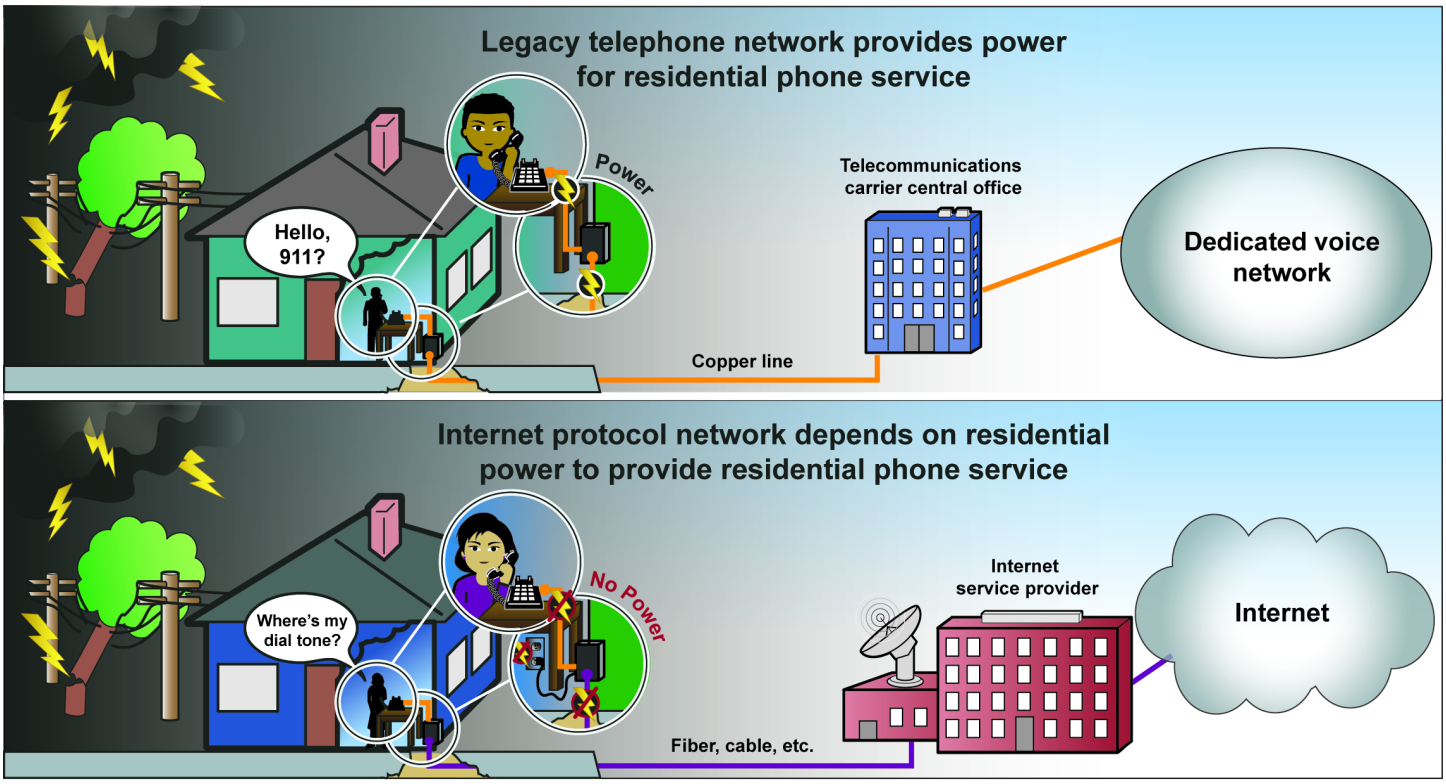
The communications sector's infrastructure is a complex system of systems that incorporates multiple technologies and services. The infrastructure includes wireline, wireless, satellite, cable, and broadcasting capabilities, and includes the transport networks that support the Internet and other key information systems. Historically, networks based on time-division multiplexed (TDM) circuit-switches[6] running on copper loops provided voice service for consumers. In a 2015 report and order, FCC noted that for over 100 years customers could rely upon telecommunications carriers for backup power for their residential landline phones during power outages[7] because power is provided over traditional copper telephone lines. In other words, telephones served by copper networks continue to work during commercial power outages as long as the telephones do not need to be plugged into an electrical outlet to function.[8] On the other hand, the physical infrastructure for IP-based networks, such as fiber and co-axial cable, does not carry power, which means telephones connected to IP networks may not work during commercial power outages (see fig.1).

[6] TDM is a method by which multiple subscribers can share a common transmission medium.

[7] *In the Matter of Technology Transitions; Policies and Rules Governing Retirement Of Copper Loops by Incumbent Local Exchange Carriers; Special Access for Price Cap Local Exchange Carriers; AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, 30 FCC Rcd 9372, August 7, 2015, Released, August 6, 2015, Adopted.

[8] For the traditional copper landline phone to continue to work during electric outages, the carrier's central office must maintain power and supply that power through an all-copper network, meaning copper has not been replaced by fiber at any point in the network between the central office and the consumer's landline phone.

**Figure 1: Legacy Copper Network versus IP Network without Backup Power during Power Outages**




Source: GAO analysis of FCC information. | GAO-16-167

According to FCC, networks other than copper and services not based on TDM may not support data-based services such as credit card readers, home alarms, and medical alert monitors. The Alarm Industry Communications Committee noted in comments filed with FCC that the traditional TDM-based telephone service meets the standards necessary for fire protection and other life and safety applications, such as line seizure, the detection of a loss in communications path, and the proper encoding and decoding of tone messages sent by the alarm panel.[9] The committee stressed that as networks transition to IP-based networks, these traits must be preserved.

[9]The Alarm Industry Communications Committee is composed of representatives of the Central Station Alarm Association International, the Electronic Security Association, the Security Industry Association, and major alarm companies and manufacturers.

FCC notes that there are a number of distinct but related kinds of technology transitions, including: (1) changes in network facilities and in particular retirement of copper facilities, and (2) changes that involve the discontinuance, impairment, or reduction of legacy services, irrespective of the network facility used to deliver those services. In the case of retiring copper facilities, the Communications Act of 1934, as amended (Communications Act), and FCC rules thereunder allow telecommunications carriers to transition to new facilities without needing FCC approval as long as the change of technology does not discontinue, reduce, or impair the services provided.[10] FCC rules do require incumbent telecommunications carriers to give notice to interconnecting carriers of planned copper retirements, and new FCC rules require incumbent carriers to give notice to retail customers of such planned copper retirements when such retirements remove copper to the customers' premises without consumer consent, along with particular consumer protection measures.[11] Such consumer protections include explanations of how consumers may seek more information from carriers about the copper retirement process and its possible impact on consumers' service, and links for the FCC's consumer complaint portal. With respect to service discontinuance, under the Communications Act, telecommunications carriers must obtain FCC approval before they discontinue, reduce, or impair service to a community or part of a community.[12] FCC regulations include procedures for carriers to discontinue, reduce, or impair service. The regulations state that to discontinue telecommunications service, carriers must notify customers of this intent and file an application with FCC. Once an application is received, FCC issues a public notice and considers these applications on a case-by-case basis and also accepts and reviews comments on proposed discontinuations, reductions, or impairments of

[10]47 U.S.C. §§ 214, 251(c)(5); 47 C.F.R. §§ 51.325-51.335.

[11]47 C.F.R. § 51.332 (as amended by *In the Matter of Technology Transitions, Policies and Rules Governing Retirement of Copper Loops by Incumbent Local Exchange Carriers, Special Access for Price Cap Local Exchange Carriers, and AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services*, 30 FCC Rcd 9372, August 7, 2015, Released, August 6, 2015, Adopted, at App'x A). The updated copper retirement rules adopted in August 2015 contain information collection requirements that must be approved by the Office of Management and Budget. FCC will publish a document in the Federal Register announcing the effective date.

[12]47 U.S.C. § 214(a).

telecommunications service.[13] According to the order, FCC will normally authorize the discontinuance, reduction, or impairment of service unless it is shown that to do so would adversely affect the public convenience and necessity, with regard to which FCC considers, among other things, whether customers would be unable to receive service or a reasonable substitute from another carrier.

FCC officials told us that there is no forcing action or requirement for telecommunications carriers to transition to IP by a certain date and that the technology transitions are organic processes without a single starting or stopping point. In an August 2015 order, FCC noted that recent data indicate 30 percent of all residential customers choose IP-based voice services from cable, fiber, and other carriers as alternatives to legacy voice services. Furthermore, an additional 44 percent of households were "wireless-only" meaning these households only have wireless telephones. The August 2015 order also states that overall, almost 75 percent of U.S. residential customers (approximately 88-million households) no longer receive telephone service over traditional copper facilities because they rely on IP-based voice services or wireless phone service.[14]

Both FCC and DHS play a role in regulating the transition to IP and ensuring public safety communications are not at risk.

- Pursuant to the Communications Act, FCC is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable throughout the United States.[15] FCC officials stated that FCC is to promote the reliability, resiliency, and availability of the nation's communications networks at all times, including in times of emergency or natural disaster. Further, FCC has the authority to adopt, administer, and enforce rules related to communications

[13]47 C.F.R. § 63.71(a).

[14]*In the Matter of Technology Transitions, Policies and Rules Governing Retirement of Copper Loops by Incumbent Local Exchange Carriers, Special Access for Price Cap Local Exchange Carriers, and AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services,* 30 FCC Rcd 9372, August 7, 2015, Released, August 6, 2015, Adopted.

[15]47 U.S.C. § 151 et seq.

reliability and security,[16] 911,[17] and emergency alerting.[18] FCC's regulations include requirements for certain telecommunications carriers to report on the reliability and security of communications infrastructures, specifically reporting on network outages. FCC also asks carriers to report voluntarily on the status of the restoration of communications in the event of a large scale disaster.

- DHS is the principal federal agency to lead, integrate, and coordinate the implementation of efforts to protect communications infrastructure. DHS's role in critical infrastructure protection is established by law and policy. The Homeland Security Act of 2002,[19] Homeland Security Presidential Directive 7,[20] and the *National Infrastructure Protection Plan*[21] establish an approach for protecting the nation's critical infrastructure sectors— including communications—that focuses on the development of public private partnerships and establishment of a

[16]*See, e.g.*, 47 U.S.C. §§ 151,154(o), 222,303(b), 303(g), and 551.

[17]*See, e.g.*, 47 U.S.C. §§ 151, 152(a), 154(i)-(j), 157, 160, 201, 214, 222, 251(e), 301, 302, 303(b), (g) and (r), 251(e)(3), 307, 307(a), 309, 309(j)(3), 316, 316(a), 332, 615 note, 615, 615a, 615a-1, 615b, and 615c(g).

[18]*See, e.g.,* 47 U.S.C §§ 151, 152, 154(i), 154(o), 301, 303(b), (g) and (r), 303(v), 307, 309, 335, 403, 544(g), 606, 613, 615 and 1302; The Warning, Alert and Response Network (WARN) Act, Title VI of the Security and Accountability for Every Port Act of 2006, Pub. L. No. 109-347, §§ 602(a), (b), (c), (d), (f), 603, 604, and 606, 120 Stat. 1884 (2006) (the "WARN Act"); Twenty-First Century Communications and Video Accessibility Act of 2010, Pub. L. No. 111-260 and Pub. L. No. 111-265.

[19]Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002). Among other things, the act assigned DHS responsibility for protecting critical infrastructure.

[20]The White House, Homeland Security Presidential Directive 7 (Washington, D.C.: Dec.17, 2003). The directive assigned responsibilities for DHS and other federal agencies focused on specific critical infrastructure sectors. These sector-specific agencies are responsible for identifying, prioritizing, and coordinating the protection of critical infrastructure to prevent, deter, and mitigate the effects of attacks. As of February 12, 2013, Presidential Policy Directive 21 revoked Homeland Security Presidential Directive 7. However, Presidential Policy Directive 21continues to assign agencies to specific sectors and states that plans developed pursuant to Homeland Security Presidential Directive 7 shall remain in effect until specifically revoked or superseded.

[21]*National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: 2013). This plan is intended to guide efforts to manage risks to the nation's critical infrastructure by identifying national priorities; articulating clear goals; mitigating risk; measuring progress; and adapting based on feedback and the changing environment.

risk management framework. These policies establish critical infrastructure sectors, including the communications sector; assign agencies to each sector (sector-specific agencies), including DHS as the sector lead for the communications and information technology sectors; and encourage private sector involvement. Pursuant to Presidential Policy Directive 21, DHS is to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure from all-hazards.[22]

## Carriers Face Challenges Preserving Services on IP Networks during Times of Crisis

As the nation's telecommunications systems transition to IP networks, carriers can face challenges during times of crisis that affect end users' ability to call 911 and receive emergency communications. These challenges include (1) preserving consumer service and (2) supporting existing emergency communications services and equipment. FCC, DHS, and other stakeholders have taken steps to help address these challenges, but some persist.

### Preserving Consumer Service

Providers face challenges in preserving service during times of crisis such as natural disasters or outages caused by malicious acts and accidents. For example, weather events, such as hurricanes and tornados, can damage telecommunications infrastructure and the power sources communications systems rely on to provide service. A 2012 DHS report entitled *2012 Risk Assessment Report for Communications* identified risks to communication networks from violent weather that include fuel not being available for generators during a commercial power outage; aerial infrastructure unable to withstand high winds; utility poles unable to withstand high winds; and underground infrastructure unable to withstand flooding. Destruction of communications infrastructure by storms can affect both legacy copper wire and IP networks. For example, in talking with officials from New York and New Jersey about Hurricane Sandy, the officials told us the storm damaged both copper lines and fiber optic cable. However, as explained previously, in general, consumers with basic telephones and service provided over copper lines can still operate during a commercial power outage, as long as the carrier's central office maintains power and keeps supplying line power through an all-copper network. In contrast, consumers with service provided over IP networks require a backup power source, such as a battery, since IP network

[22]Presidential Policy Directive/PPD-21—Critical Infrastructure Security and Resilience (Washington, D.C.: Feb. 12, 2013).

infrastructure does not carry electrical power for the purpose of powering end devices, such as telephones. Officials we contacted from four state agencies, and representatives from four trade and industry organizations and consumer groups emphasized the importance of backup power for communications during emergencies.

To address backup power requirements during a commercial power outage, FCC issued rules addressing 911 reliability and the reliability and continuity of communications networks for both carriers' central office facilities and consumers' homes. Specifically, in 2013, FCC issued new rules on central office backup power certification requirements for certain 911 service providers.[23] In an August 2015 order, FCC noted that many consumers remained unaware they needed to take action to ensure their landline telephone service remained available in the event of a commercial power outage. FCC concluded that the transition to all-IP networks had the potential to create a widespread public safety issue if unaddressed. Therefore, FCC adopted rules to help ensure consumers have the information and tools necessary to maintain landline home telephone service during emergencies. When these rules become effective, FCC will require that telecommunications carriers communicate information to consumers regarding backup power, such as the availability of backup power sources, service limitations with and without backup power, and purchase options. FCC will also require telecommunications carriers to give consumers the option to purchase a backup power device with at least 8 hours of standby power during a commercial power outage enabling calls, including those to 911. Furthermore, FCC will require carriers to offer consumers the option to purchase 24 hours of backup power within 3 years.[24]

In addition to weather events, telecommunication network outages can occur through malicious acts, such as vandalism and cyber attacks, and

[23]This order addresses, among other things, annual audits of critical circuit diversity, 911 network monitoring, and specific time limits for outage notifications to 911 call centers. *In the Matter of Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, Report and Order, FCC 13-158, 28 FCC Rcd. 17476 (2013). And *In the Matters of Improving 911 Reliability and Reliability and Continuity of Communications Networks Including Broadband Technologies.* Order on Reconsideration, 30 FCC Rcd 8650, July 30, 2015, Released, July 29, 2015, Adopted. (2015).

[24]*In the Matter of Ensuring Continuity of 911 Communications,* FCC 15-98, 30 FCC Rcd 8677, August 7, 2015, Released, August 6, 2015, Adopted.

by accidental cable cuts and software coding errors. For example, a fiber optic cable north of Phoenix was vandalized in February 2015, causing large-scale telephone and Internet outages across much of Northern Arizona. According to local officials we contacted, the outage lasted about a day and included Flagstaff, Sedona, Prescott, and surrounding areas potentially affecting more than 300,000 people. Officials told us that the Flagstaff police department's 911 lines were down, so they sent staff to a backup site at the Arizona Department of Public Safety to answer calls; the police department also lost all Internet, a loss that prevented it from checking for warrants and driver's licenses. Additionally, officials told us that some businesses closed because they could not process credit card transactions, that ATMs did not work, and that Northern Arizona University lost Internet service. According to a Flagstaff official, the telecommunications carrier is now building, and expects to complete by 2016, an additional fiber optic cable that will improve resiliency and redundancy.

Cyber attacks can also challenge both IP networks and traditional legacy networks; however, DHS officials told us that IP networks are more prone to cyber attacks than legacy networks, because legacy networks are closed systems that are less vulnerable to cyber attacks. Under the terms of a 2013 executive order and a related presidential policy directive, it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats.[25] In a 2015 report, the Communications Security, Reliability and Interoperability Council (CSRIC)[26] identified cybersecurity threats to Voice over IP (VoIP)[27] and voice services that include disrupting network availability,

[25]On February 12, 2013, the President signed Executive Order 13636 and issued Presidential Policy Directive 21 to improve critical infrastructure cybersecurity and advance efforts to strengthen and maintain secure, functioning, and resilient critical infrastructure, respectively. The executive order, which was published in the *Federal Register* at 78 Fed. Reg. 11739 (Feb.19, 2013), prescribes actions to be taken by federal agencies, including the Departments of Defense, Homeland Security, and Commerce (including the National Institute of Standards and Technology), related to enhancing cybersecurity. In addition, the directive details responsibilities of federal agencies related to critical infrastructure security and resilience, including those of FCC and the Department of Commerce.

[26]CSRIC is one of FCC's federal advisory committees and is composed of experts from the private sector, consumer or community organizations or other non-profit entities, and representatives from federal and other government agencies.

[27]VoIP is the routing of voice conversations over the Internet or any other IP network.

compromising confidentiality, and spoofing a caller's identity.[28] According to FCC officials, CSRIC is developing recommendations to support the real-time sharing of cyber threat information among private sector entities. For our recent products related to cybersecurity and information security, see related GAO products listed at the end of this report.

As with legacy copper networks, accidents also cause IP network outages affecting communication capabilities. For example, a truck accident in 2014 took out 400 feet of aerial fiber optic cable along a rural road in Mendocino County, California. According to a local incident report, telephone, Internet, cellular, and 911 services went down for thousands of residents, and Internet service was out almost completely along a 40-mile corridor for approximately 45 hours. According to local officials we contacted, 911 services were unavailable, and the county sheriff estimated that 20 percent of county residents lost vital services. Alert notifications through phone calls were unavailable for residents waiting to receive evacuation notices just as a nearby wildfire was growing.[29] According to an incident report, health care providers could not be reached; banks and supermarkets closed because they were unable to function without Internet, telephone, and ATM services; and electronic food stamp benefits were unavailable.

IP network outages caused by human error, such as software coding errors, can affect large numbers of people over wide geographic areas. Such outages are sometimes referred to as "sunny day" outages. For example, in April 2014, a 911 call-routing facility in Colorado stopped directing emergency calls to 911 call centers in 7 states.[30] The outage was caused by a coding error and resulted in a loss of 911 services for more than 11-million people for up to 6 hours. Unlike legacy copper networks, IP networks permit call control to be distributed among just a few large servers nationwide, meaning each server can serve millions, or

[28]CSRIC Working Group 4, *Cybersecurity Risk Management and Best Practices: Final Report,* (Washington, D.C.: March 2015).

[29]According to the California Public Utilities Commission, reverse calling alert notification (commonly referred to as Reverse 911) is used in California to inform residents and give emergency instructions during fires, flooding, extreme weather, or any other kind of emergency.

[30]According to FCC, over 6,600 calls to 911 did not reach the appropriate call center across seven states including Washington, North Carolina, South Carolina, Pennsylvania, California, Minnesota, and Florida.

even tens of millions, of customers, according to FCC. State officials from New York and California told us that IP networks allow for increased consolidation of equipment and facilities, which means that when an outage does occur, it can potentially last longer and affect more people across a wider area than legacy networks. An FCC investigation into a multistate 911 outage in 2014 found that this geographical consolidation of critical 911 capabilities may increase the risk of a large "sunny day" outage caused by software failures rather than disasters or weather conditions.[31] According to this investigation, large-scale outages may result when IP networks do not include appropriate safeguards. In 2013, FCC adopted rules requiring 911 service providers to certify annually that they comply with industry-backed best practices or implement alternative measures that are reasonably sufficient to assure reliable 911 service.[32]

### Supporting Existing Emergency Communication Services and Equipment

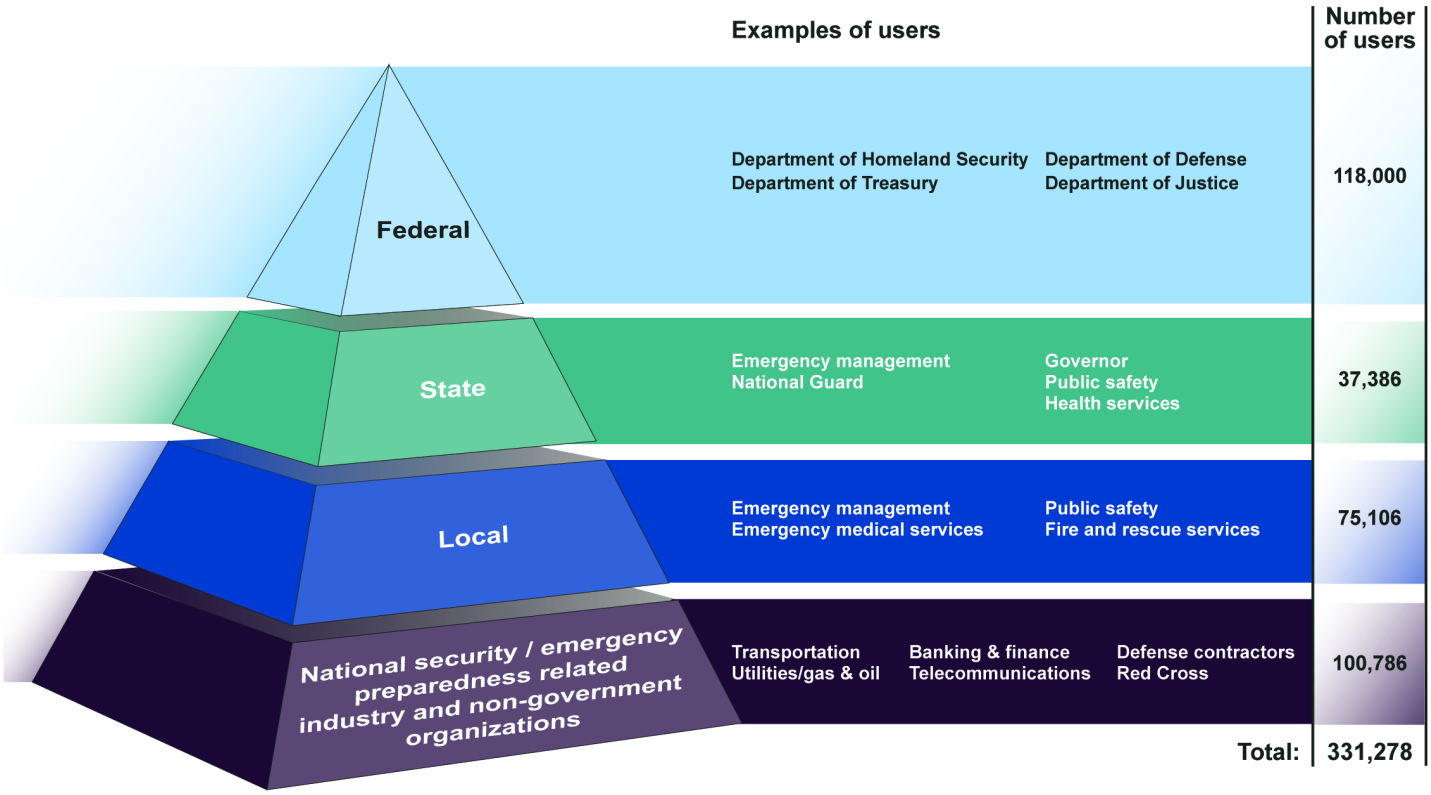
IP networks may not support existing communication services that key government officials and others rely on during times of crisis. Communications networks can become congested during emergencies, preventing government officials and other national security and emergency preparedness personnel from communicating with one another. To overcome this congestion, DHS maintains priority telecommunications services, such as the Government Emergency Telecommunications Service (GETS) that provide priority calling capabilities to authorized users. GETS was initially designed in the 1990s to operate with legacy networks during times of congestion. DHS officials told us that over the past 5 years similar priority features have been implemented in the core IP networks of select U.S. nationwide long-distance service providers. DHS officials told us congestion, caused by high-call volume and potentially as a result of cyber attack, will continue to be a challenge in an IP environment. FCC officials told us that although congestion may not be as likely in IP networks as it was in legacy networks, it will still occur. As shown in figure 2, numerous government

[31]FCC, Public Safety & Homeland Security Bureau, *April 2014 Multistate 911 Outage: Cause and Impact*, PS Docket No. 14-72, PSHSB Case File Nos. 14-CCR-0001-0007 (October 2014).

[32]*In the Matter of Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, Report and Order 28 FCC Rcd 17476, December 12,2013, Released, December 12,2013, Adopted.

officials and non-government organizations in critical positions rely on GETS when networks become congested during times of crisis.[33]

**Figure 2: Government Emergency Telecommunications Service (GETS) Users, as of November 2015**




Source: Department of Homeland Security. | GAO-16-167

The value of priority telecommunications service when compared to regular network performance becomes apparent during times of crisis. For example, according to DHS, during Hurricane Sandy and the immediate aftermath, networks were congested due to damage and high call volume into and out of the storm-damaged area. Likewise, according

[33]In addition, tribal and territorial government officials, critical infrastructure sectors in industry, and non-governmental organizations performing their national security and emergency preparedness missions are eligible to use GETS.

to DHS officials and a DHS report on the Boston Marathon bombing, as news of the bombs spread, cell phone networks became congested with users and were largely unavailable for about 90 minutes.[34] As shown in table 1, GETS had high call-completion rates during recent times of crisis.

**Table 1: Government Emergency Telecommunications Service (GETS) Performance during Select Crises**

| Event | GETS calls | GETS completion rate |
|---|---|---|
| Hurricane Sandy, October 2012 | 18,347 | 99.4% |
| Boston Marathon bombing, April 2013 | 291 | 97.3% |
| Oklahoma tornadoes, May 2013 | 636 | 95.8% |
| California wildfires, May 2014 | 1,629 | 98% |

Source: Department of Homeland Security. | GAO-16-167

DHS officials told us that the current GETS will likely lose some functionality during the transition to an all-IP environment.[35] The officials said they are planning a project that will provide priority for IP wireline access, but the project has not yet received approval for acquisition. In 2015, a multi-agency executive committee reported that the national security and emergency preparedness community must be able to rely on these priority services to complete their mission-essential communications in the IP environment.[36] DHS is working on a program that is aimed at enabling users to have priority voice, data, and video communications as networks evolve, but according to DHS officials, data and video capabilities will not be available for several years. In the meantime, as telecommunications carriers transition from legacy networks to IP networks, key national security and emergency preparedness personnel might not be able to complete important GETS calls during times of crisis. CSRIC is currently assessing how priority

[34]Specific data on call completion rates for callers not using GETS was not available.

[35]Under legacy systems, each GETS call is routed with priority through three networks—an access network, a long-distance network, and an egress network. In an IP system, a GETS call currently receives priority on the long-distance core network but not on the access or egress networks, according to DHS.

[36]The National Security Emergency Preparedness Communications Executive Committee is an interagency forum to address such communication matters for the nation. Its members represent the Departments of State, Defense, Justice, Commerce, and Homeland Security, the Office of the Director of National Intelligence, the General Services Administration, and FCC.

services programs can take advantage of IP technologies and intends to recommend protocols that can be used to ensure priority communications upon the retirement of legacy services. As CSRIC noted, this is important since the federal government is losing priority capabilities that rely on networks that will eventually be replaced by IP-based infrastructure. According to FCC officials, CSRIC estimates that the recommendations on protocols and standards that can support the delivery of priority communications for first responders and national security personnel over IP networks will be complete in March 2017.

New IP networks may no longer support other government and consumer public safety services and equipment that work in the existing legacy network. Examples of such items include alarm systems and 911 call center systems. According to the Alarm Industry Communications Committee, telecommunications carriers installing new IP services may prevent alarm signals from being transmitted, and some IP services may improperly encode alarm signals. In comments submitted to FCC, the Association of Public Safety Communications Officials International (APCO) noted that alarm systems and medical alert monitors need to be provided for under new IP networks. APCO commented that alarms and alerts are a critical part of the input into 911 call centers and any identified shortfalls or anomalies should be identified to ensure that any effect to the public or public safety is known well ahead of time. APCO also commented that copper replacements in the foreseeable future must accommodate existing 911 call centers in the relevant service area, including those that have not yet transitioned to IP-based systems. As discussed, that transition will not be immediate and continuity of operations with existing 911 systems is vital for public safety.

# Agencies and Stakeholders Have Taken Steps to Ensure IP Networks Are Reliable, but FCC Has Little Information to Assess the Effect of the IP Transition

## Efforts to Ensure the Reliability of IP Networks

### FCC Efforts

In addition to addressing the specific challenges affecting IP networks during times of crisis described above, FCC has taken a variety of other actions to help ensure the overall reliability of IP networks, including the following:

- *Proposed criteria in August 2015 to evaluate and compare the replacement of legacy services*. FCC had not previously codified any specific criteria by which it evaluated the adequacy of substitute services, but proposed changes to the process in a further notice of proposed rulemaking.[37] Specifically, FCC proposed that to be eligible for automatic grant of authority under FCC's rules, a telecommunications carrier seeking to discontinue an existing retail service must demonstrate that any substitute service meet criteria related to (1) interoperability with devices and services, such as alarm services and medical monitoring; (2) support for 911 services and call centers; (3) network capacity and reliability; (4) quality of both voice service and Internet access; (5) access for people with disabilities, including compatibility with assistive technologies; (6) network security

[37] *In the Matter of Technology Transitions, Policies and Rules Governing Retirement of Copper Loops by Incumbent Local Exchange Carriers, Special Access for Price Cap Local Exchange Carriers, and AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services,* 30 FCC Rcd 9372, August 7, 2015, Released, August 6, 2015, Adopted.

in an IP-supported network; (7) service functionality; and (8) coverage throughout the service area. In addition, FCC proposed to require that part of the evaluation to discontinue a legacy retail service should include whether the carrier has an adequate consumer education and outreach plan. FCC noted it believes establishing these criteria will benefit industry and consumers alike and will minimize complications when carriers seek approval for large scale discontinuances. It also noted that having clear criteria in place will better allow carriers to know how they can obtain approval for discontinuing legacy service once they are ready to do so. According to representatives from Public Knowledge, this organization had urged FCC to establish metrics to compare the services that carriers are discontinuing with replacement services.[38] The organization's representatives noted that without ensuring new services are actually substitutes for the services being phased out, there is a risk that entire communities could lose critical functionality in their communications networks. In the further notice of proposed rulemaking, FCC tentatively concluded that several of the criteria proposed by Public Knowledge are the appropriate criteria.

- *Updated copper retirement rules and definitions to help ensure the public has the information needed to adapt to an evolving communications environment*. FCC issued new rules in an August 2015 report and order that, among other things, require incumbent carriers to directly notify consumers of plans to retire copper networks to the customer's premises without customer consent. In this report and order, FCC also updated its definition of copper retirement due to the frequency and scope of copper network retirement. Included in this definition is *de facto* retirement, i.e., the failure to maintain these copper lines that is the functional equivalent of removal or disabling. FCC noted that it made these changes in rules and definitions since the record developed in that proceeding reflects numerous instances in which notice of copper retirement has been lacking, leading to

[38]Public Knowledge represents the public interest on a variety of issues including telecommunications and consumer rights.

consumer confusion, and therefore consumers need direct notice for these important network changes that may directly affect them.[39]

- *Collected and analyzed network outage data, looking for trends, and communicated with telecommunications carriers*. FCC developed and maintains the Network Outage Reporting System (NORS) for collecting confidential outage information from telecommunications carriers. These carriers are required to report information about disruptions or outages to their communications systems that meet specified thresholds.[40] According to FCC, engineers on its staff monitor and analyze the outage reports in real time looking for trends in outages, communicate with carriers about outages, and produce a high-level network outage report. FCC officials told us that even though the outage information is not publicly reported, they believe the act of reporting helps network providers correct problems and that by combining multiple reports, FCC gains insight on network reliability and working with carriers cooperatively leads to better outcomes with fewer, less severe outages.[41] FCC shares NORS reports with DHS's Office of Emergency Communications, which may provide information from those reports to such other governmental authorities as it may deem to be appropriate.[42] Otherwise, reports filed in NORS are presumed confidential and are thus withheld from routine public inspection.[43] However, in March 2015, FCC proposed, among other

[39]*In the Matter of Technology Transitions, Policies and Rules Governing Retirement of Copper Loops by Incumbent Local Exchange Carriers, Special Access for Price Cap Local Exchange Carriers, and AT&T Corporation Petition for Rulemaking to Reform Regulation of Incumbent Local Exchange Carrier Rates for Interstate Special Access Services,* 30 FCC Rcd 9372, August 7, 2015, Released, August 6, 2015, Adopted. According to FCC officials, most of the copper retirement rules adopted in this order contain information collection requirements that must be approved by the Office of Management and Budget.

[40]47 C.F.R. § 4.5. Such outages are defined as those that meet a minimum threshold of 900,000 user minutes, which are calculated by multiplying the number of affected users by the length of the outage. For example, an outage that affected 30,000 users for a minimum of 30 minutes would meet the threshold of 900,000 user minutes.

[41]We did not obtain NORS data because we would not be able to report publicly on the confidential outage data.

[42]*In the Matter of New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, 19 FCC Rcd 16830 (2004), August 19, 2004, Released, August 4, 2004,Adopted.

[43]47 C.F.R. § 4.2.

things, granting states read-only access to those portions of the NORS database that pertain to communications outages in their respective states to advance compelling state interests in protecting public health and safety.[44] Representatives from two state agencies and two consumer organizations we contacted told us that granting states access to outage reports would improve the overall reliability of communications networks by giving them additional information.

- *Tracked the status of the restoration of communications in the event of a large scale disaster*. FCC developed and maintains the Disaster Information Reporting System (DIRS), a voluntary system used by members of the communications sector intended to provide information on the status of restoration efforts to FCC and DHS. DIRS reports include information on major equipment failures and the service and geographic area affected. According to FCC officials, DIRS is only activated during major disasters, and since these incidents are unique, the system is not designed to track trends. For example, the officials said that DIRS is often activated during hurricanes, but because of differences in wind speed, direction, and other challenges, outages from one hurricane do not necessarily indicate infrastructure will be affected the same way in another hurricane.

- *Chartered CSRIC to provide FCC with recommendations on ways to improve security, reliability, and interoperability of communications systems*. FCC officials told us CSRIC has not specifically looked at ways to improve reliability of IP networks; however, there have been a number of working groups that aim to improve the overall reliability of telecommunications networks. Specifically, in September 2014, CSRIC issued a report and series of best practices for providing backup power to customers relying on IP networks and on consumer notification.[45]

[44]*In the Matter of Amendments to Part 4 of the Commission's Rules Concerning Disruptions to Communications; New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, 30 FCC Rcd 3206, March 30, 2015, Released, March 27, 2015, Adopted. FCC also sought comment on proposals to revise network outage reporting rules, including raising the threshold for reporting major outages, partial 911 outages, new metrics to measure congestion during emergencies, and reducing the time to resolve certain events.

[45]CSRIC Working Group 10B, *CPE Powering – Best Practices: Final Report* (Washington, D.C.: September 2014).

## DHS Efforts

DHS has also taken the following actions to help ensure the reliability of IP networks during times of crisis:

- *Coordinated with other federal government agencies, owners and operators of communications networks, and state, local, tribal, and territorial governments*. As the Sector Specific Agency for the communications sector, DHS manages the industry-government relationship, encourages private sector involvement through the involvement of the sector-coordinating councils, and maintains the *Communications Sector Specific Plan*. According to representatives of the Communications Sector Coordinating Council, the Council works closely with DHS, and they noted DHS is helpful in providing assistance for educational and outreach programs, including ensuring training opportunities occur when needed. DHS also coordinates with stakeholders by participating in CSRIC and by coordinating and serving as the Executive Secretariat support to the President's National Security Telecommunications Advisory Committee—a presidential advisory group comprised of chief executives from major telecommunications companies, network service providers, and the information technology, and aerospace industries.[46] Additionally, DHS's Office of Emergency Communications provides coordination support by offering training, coordination, and tools to stakeholders.

- *Coordinated the development and implementation of the 2010 Communications Sector Specific Plan and is currently working on an updated plan*.[47] The sector specific plan was developed by DHS, the Communications Sector Coordinating Council, and the Government Communications Coordinating Council and is intended to ensure the sector effectively coordinates with sector partners, other sectors, and DHS. According to representatives of the Communications Sector Coordinating Council, they met regularly with DHS to update the sector specific plan. The plan provides a framework for industry and government partners to establish a coordinated strategy to protect the nation's critical communications infrastructure. Part of this framework includes conducting national risk assessments. With respect to

[46]The group aims to develop recommendations to the President to assure vital telecommunications links through any event or crisis and to help the U.S. government maintain a reliable, secure, and resilient national communications posture.

[47]DHS, *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (2010).

communications, DHS issued a report entitled *2012 Risk Assessment Report for Communications*, which according to the report, represents the culmination of a 2-year period during which 29 government and 32 industry sector partners assessed physical, cyber, and human risks of concern that could potentially affect local, regional, and national communications. According to DHS officials, the Communications Sector Coordinating Council and Government Communications Coordinating Council determined an updated risk assessment was not needed because details of the changing risk environment will be discussed and updated in other sector documents, such as the sector specific plan. DHS officials also told us the new plan should be completed in 2015 and will be updated to include the communications sector's transition to IP networks and will include more focus on cybersecurity-related content. We did not evaluate the 2010 plan because it was being updated and did not evaluate the 2015 plan because it was not issued at the time of our review.

- *Coordinated the development of the 2014 National Emergency Communications Plan*.[48] This plan aims to enhance emergency communications capabilities at all levels of government in coordination with the private sector, nongovernmental organizations, and communities. DHS developed recommendations to help meet the plan's five broad goals related to (1) governance and leadership, (2) planning and procedures, (3) training and exercises, (4) operational coordination, and (5) research and development. According to the plan, DHS's Office of Emergency Communications intends to coordinate with public safety agencies and emergency responders and will identify strategies and timelines to accomplish the plan's goals, objectives, and recommendations and measure progress nationwide.[49]

### Telecommunications Carrier's Efforts

In the private sector, telecommunications carriers have also worked to ensure their IP networks are functional during times of crisis in the following ways:

- *Built resiliency and reliability into IP networks as part of business operations and planning for emergencies*. According to DHS, as the owners and operators of the majority of the nation's communications

[48]DHS, *National Emergency Communications Plan* (Washington, D.C.: November 2014).

[49]The plan includes recommendations on updating the priority service programs (including GETS) to help them successfully migrate to IP enabled fixed and mobile broadband networks.

networks, private sector entities are responsible for protecting key commercial communications assets, as well as ensuring the resiliency and reliability of communications during day-to-day operations and emergency response and recovery efforts. In addition, commercial communications carriers have a primary role in network restoration during outages and service failures and support reconstitution for emergency response and recovery operations. Representatives of the three largest telecommunication carriers told us they are taking action at the company level to improve reliability because building reliability and resilience into networks are part of normal business operations. For example, these carriers have developed emergency preparedness plans for events such as hurricanes, to help ensure network reliability. These plans included pole replacement, decreased dependency on aerial facilities, and adding additional generators. Officials from one major carrier told us that customers expect the phone to work when they pick it up to make a call and that the company risks losing customers if it cannot provide reliable service.

- *Participate in a variety of groups intended to provide information and improve the overall reliability of communications networks*. For example, in addition to groups like CSRIC and the Communications Sector Coordinating Council described above, telecommunications carriers participate in other organizations such as the Alliance for Telecommunications Industry Solutions (ATIS).[50] ATIS's Network Reliability Steering Committee advises the communications industry through developing and issuing standards, technical requirements and reports, best practices, and annual reports. ATIS also launched a task force looking at how the IP transition affects public safety communications infrastructure.

## Selected State Agency Efforts

State authorities from three public utility agencies told us that they have taken action to ensure the reliability of IP networks. These actions include collecting consumer complaints, levying fines, reviewing outage data, and making recommendations for improvement. For example, officials at one state agency told us that they receive and investigate complaints and if an issue is identified levy fines or open a rulemaking proceeding. Officials at another state agency told us they review outage data and make recommendations for improvements based on lessons learned. According

[50]ATIS is a technical planning and standards organization with members from communications companies working to develop and promote technical and operational standards.

to the DHS's 2010 Sector Specific Plan, the state Public Utility Commission is the primary authority for implementing regulations, and individual telecommunications carriers work directly with state authorities regularly to address regulatory issues. However, according to the National Regulatory Research Institute, more than half the states have made changes to their regulatory authority that reduced or eliminated retail telecommunications regulation.[51] For example, one state agency told us that although the commission previously had a role in ensuring the reliability and robustness of the communications network, it no longer has that authority.

## Although FCC Has Data Collection Efforts Under Way, It Has Limited Information about the Effect of the IP Transition

FCC is collecting data on the IP transition and sought comment on collecting additional data on the transition's effect on consumers, but could do more to ensure it has the information it needs to make data-driven decisions about the IP transition.[52] The primary way FCC intends to gather information about the IP transition is through service-based experiments. In particular, FCC established a framework in January 2014 within which carriers can conduct voluntary service-based experiments.[53] These voluntary experiments would allow telecommunications carriers to substitute new communications technologies for the legacy services over copper lines that they are currently providing to customers and to test a variety of approaches to resolving operational challenges that result from transitioning to new technology and that may affect users. According to FCC, these experiments are not intended to test technologies or resolve legal or policy debates.

[51]The National Regulatory Research Institute is the research arm of National Association of Regulatory Utility Commissioners. National Regulatory Research Institute, *Telecommunications Legislation 2014: Completing the Process,* Report No. 14-07 (Silver Spring, MD: June 2014).

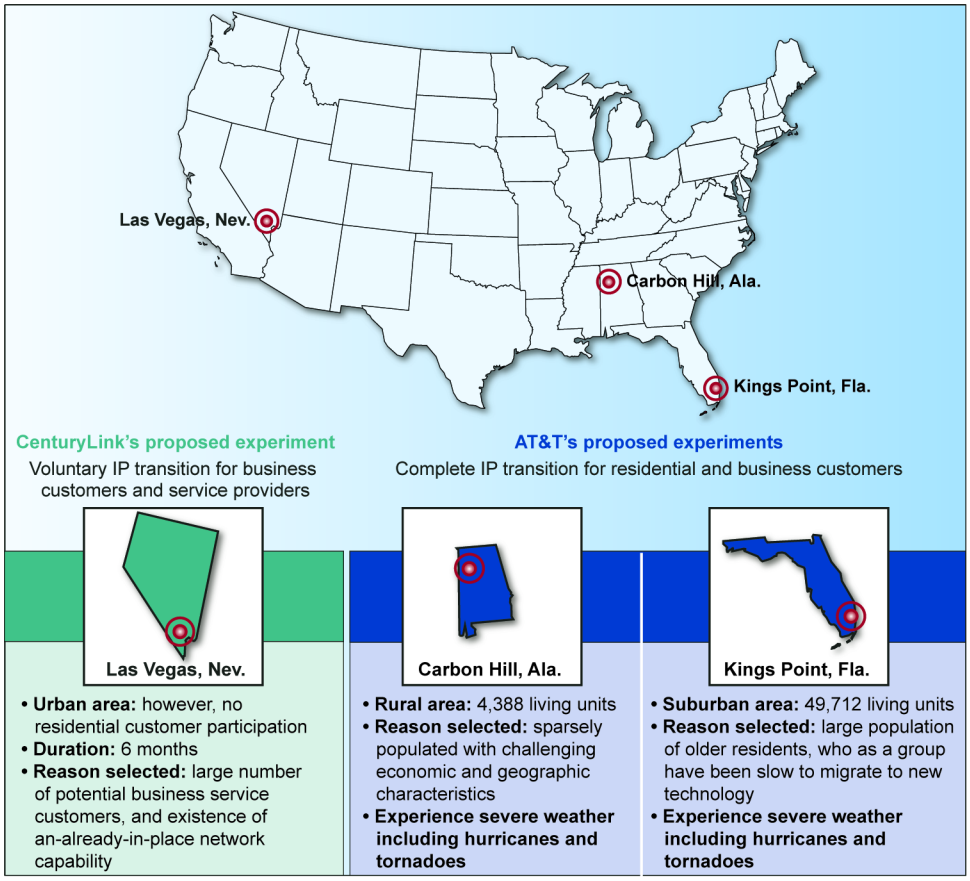
[52]In January 2014, FCC sought comment on how it could supplement its data-gathering process on the IP transition, with comments due in March 2014 and reply comments due in April 2014. According to FCC officials, while the formal comment period has closed, FCC was still accepting filings at the time of our review.

[53]*In the Matter of Technology Transitions; AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition; Connect America Fund; Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services And Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; Numbering Policies for Modern Communications*: 29 FCC Rcd 1433, January 31, 2014, Released, January 30, 2014, Adopted.

FCC established technical parameters for each experiment, including requiring each proposal to provide sufficiently detailed information about how the experiments will be designed to allow meaningful public comment and thorough evaluation of the proposed experiment. Specifically, each experiment proposal must include other information such as: the purpose and proposed metrics for measuring success; the scope of the experiment (geography, product, or service offering); the technical parameters including a description of any physical or network changes and how the experiment will affect customers and other providers and product or service offerings; and timelines. FCC noted it would find useful experiments that collect and provide data on key attributes of IP-based services, such as network capacity, 911 services and call centers, and cybersecurity. According to FCC officials, the voluntary experiments can begin without FCC approval; however, carriers planning to discontinue service have to seek permission from FCC prior to doing so. At the time of our review, the experiments were still in the early stages, and FCC had not approved the discontinuation of any existing services.

As shown in figure 3, at the time of our review, AT&T proposed experiments in two locations and CenturyLink proposed one location.

**Figure 3: Proposed Service-Based Experiments for the Internet Protocol (IP)Transition, as of October 2015**




Sources: GAO analysis of industry information and Map Resources (map). | GAO-16-167

According to AT&T documents, initially AT&T plans to encourage voluntary migration to IP-based services for existing customers through outreach and education. Subsequently, AT&T plans to seek FCC approval to "grandfather" existing customers and offer only wireless and wireline IP-based services for new orders. The documents also note that eventually, those existing customers will also have to transition to such alternatives, but not until FCC has evaluated the results and approved AT&T to discontinue legacy service and move forward to the full IP transition. As part of the trials, AT&T plans on collecting and reporting to FCC information including data on the progress of the experiment, customer complaints, network performance, call quality, and issues relating to access by persons with disabilities. According to FCC officials,

FCC intends to contract with a major research organization to collect and analyze data from the AT&T experiment locations. At the time of our review, FCC officials told us this data collection is expected to begin in several months.

Unlike the AT&T experiments, CenturyLink submitted a proposal that does not directly affect consumers. Instead this experiment focuses on business end users and service providers, and according to CenturyLink's own proposal, the experiment would be very narrow in scope. CenturyLink also noted that it was not seeking to discontinue any services or requesting a waiver of any FCC rules, even for the purposes of the experiment.

FCC is taking and plans to take additional steps to collect information on how consumers are experiencing the IP transition. FCC officials said they have begun taking action to improve consumer complaint data and make them more transparent, including launching a new consumer help center intended to collect additional consumer complaint data and working with various groups to share this and other data. FCC also plans to work with state, local, and tribal governments to leverage existing data-collection efforts and develop common definitions, categories, and a metric that will allow for comparison of consumer experiences in different parts of the country and help create a more comprehensive picture of the consumer experience as networks transition. FCC sought comment on how it could supplement its data-gathering process on the effects of technology transitions beyond consumer complaints and inquiries.

In light of the scale of the IP transition and the potential for disruptions to consumers and public safety, FCC recognizes it will need information on the effects of the transition to ensure IP communications networks are reliable. Federal standards for internal control, which provide the overall framework for identifying and addressing major performance and management challenges, stress the importance of obtaining information from external sources that may have a significant impact on an agency achieving its goals.[54] Furthermore, in its January 2014 order, FCC noted that one of its statutory responsibilities is to ensure that its core values, including public safety and consumer protection, endure as the nation

[54]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

transitions to modernized communications networks.[55] In the order, FCC noted that fulfilling this responsibility requires that FCC learn more about how the modernization of communications networks affects consumers. The order also states that FCC intends to collect data through the service-based experiments that would permit the making of data-driven decisions about the IP transition. However, it is unclear if FCC will be able to make data-driven decisions about the IP transition because of the limited number and scale of the proposed experiments. For example, one major carrier did not propose any experiments. Furthermore, as some organizations have commented, AT&T's experiments have limitations including the small number of experiments; a lack of geographic dispersion; and a lack of diverse population densities, demographics, and climates. These experiments, as planned, will affect less than 55,000 living units combined, which according to Public Knowledge, likely represent approximately 0.07 percent of AT&T's wireline customers. Additionally, the proposed experiments do not include high-density urban areas; areas with colder climates or mountainous terrains; or areas that encompass diverse populations. Finally, none of the proposed experimental areas includes critical national security or public safety locations, such as those serving Department of Defense or Federal Aviation Administration facilities.

FCC's other efforts related to data collection on the IP transition include enhancing consumer complaint data, leveraging existing data collection efforts at the state and local level, and seeking comments on how FCC could supplement its data-gathering process. However, it remains unclear if FCC can meet its information needs through these efforts. For example, as noted above, DHS officials expressed concerns about the priority services that national security and emergency preparedness personnel rely on during times of crisis, such as GETS, losing functionality in an IP environment. FCC may need additional information to help ensure that such personnel can continue to make important calls during times of crisis. Another area of uncertainty with the IP transition is the availability of 911 services and compatibility with medical devices and other

[55]*In the Matter of Technology Transitions; AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition; Connect America Fund; Structure and Practices of the Video Relay Service Program; Telecommunications Relay Services And Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities; Numbering Policies for Modern Communications*: 29 FCC Rcd 1433, January 31, 2014, Released, January 30, 2014, Adopted.

equipment. In particular, according to AT&T, in its proposed experimental areas, approximately a third of customers who chose not to migrate to wireless service expressed concerns regarding 911 calls and compatibility with medical devices and other equipment. Furthermore, FCC's solicitation of comments about the data-gathering process may not necessarily result in a change in FCC's existing policies. Although FCC's efforts to collect data represent a good start, we found FCC lacks a detailed strategy that outlines how it will address its remaining information needs, including determining what information from states and localities is available to be leveraged, a methodology for obtaining that information, and the resources required. As a result, FCC cannot ensure that it has the information necessary to make data-driven decisions about the IP transition.

## Conclusions

FCC has recognized the importance of collecting data that would enable it to make data-driven decisions about the IP transition and has sought comment on how it could supplement its data-gathering process. Nevertheless, at the time of our review, FCC had little information on the effect of the transition, namely because the service-based experiments—FCC's primary method for collecting data on the transition—were very limited in number and scale, did not cover consumer services in urban areas, and did not include critical national security or public safety locations. Although FCC has other data collection efforts under way, it is unclear whether FCC's efforts will address its remaining information needs, especially those related to the functionality of priority services and 911 availability. Developing a strategy for collecting information about how the IP transition affects public safety and consumers would help FCC address these areas of uncertainty as it oversees the IP transition and enable FCC to make data-driven decisions.

## Recommendation for Agency Action

To strengthen FCC's data collection efforts, the Chairman of FCC should develop a strategy to gather additional information on the IP transition to assess the transition's potential effects on public safety and consumers.

## Agency Comments and Our Evaluation

We provided a draft of this report to FCC and DHS for their review and comment. FCC provided written comments, reproduced in appendix II and technical comments, which we incorporated as appropriate. DHS provided technical comments, which we incorporated as appropriate.

In written comments, FCC did not state whether it agreed or disagreed with our recommendation that it develop a strategy to gather additional information on the IP transition to assess the transition's potential effects on public safety and consumers. FCC stated that it agreed with us about the importance of ensuring an informed, data-driven process for determining which services can be seamlessly supported during the IP transition, which services will need to be transformed, and which services will no longer be supported in an IP world, while preserving FCC's core functions of public safety, universal service, competition, and consumer protection. FCC noted that it is essential that it have sufficient information to make informed decisions and further stated that it has a comprehensive data strategy in place to oversee the IP transition.[56] According to FCC, its strategy for overseeing the transition combines traditional regulatory approaches with innovative methods that match the dynamism of the communications environment. FCC stated that the service-based experiments are by no means the sole means by which FCC is overseeing the IP transition and provided examples of actions it has taken to oversee the transition. For example, FCC stated that it took the following actions, which we had already highlighted in our report:

- enhanced its notification process for retirement of copper facilities;
- provided clear direction to industry concerning the circumstances in which approval must be sought before removing a service from the marketplace;
- collected NORS disruption data; and
- engaged with the private sector and other relevant stakeholders through FCC's federal advisory committees, including CSRIC.

In the letter, FCC also stated that it had taken action on some issues that were outside the scope of our review, including revising information it obtains from states on the states' collection and use of 911 fees and maintaining a "Text-to-911 Registry."

[56]As noted in our report, the communications sector's infrastructure is in the midst of a significant change, which FCC refers to as a series of technology transitions. In this report, we refer to this change as the IP transition.

While these actions are useful for FCC to oversee the IP transition, we continue to believe that FCC needs to develop a strategy to gather additional information on the potential effects of the IP transition. Especially with respect to the priority services that national security and emergency preparedness personnel rely on during times of crisis, by having a strategy to collect additional information on the IP transition, FCC could help ensure that such personnel can continue to make important calls during times of crisis. Furthermore, as AT&T noted, some residential customers have expressed concerns regarding 911 availability and compatibility with medical devices and other equipment in an IP environment. Developing a strategy to collect additional information on the transition's effects could help FCC address these areas of uncertainty.

We are sending copies of this report to the Chairman of FCC, the Secretary of Homeland Security, and appropriate congressional committees. In addition, the report is available at no charge on GAO's website at http://www.gao.gov.

If you or members of 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. Major contributors to this report are listed in appendix III.

Mark L. Goldstein
Director, Physical Infrastructure Issues

# Appendix I: Objectives, Scope, and Methodology

This report examines the reliability of the nation's communications networks in an Internet Protocol (IP) environment. Specifically, we reviewed (1) the potential challenges affecting IP networks during times of crisis and how the challenges affect end users, and (2) the actions FCC, DHS, and other stakeholders have taken to ensure the reliability of IP communications during times of crisis.

To identify challenges affecting IP networks and how the challenges affect end users, we reviewed relevant documents from the Federal Communications Commission (FCC) and Department of Homeland Security (DHS) including orders, notices and proposed rulemakings, reports, and risk assessments, as well as relevant statutes and regulations. We reviewed comments filed with FCC regarding the IP transition and emergency communications. To ensure we reviewed a broad range of comments, we selected comments by stakeholders that represented a variety of interests, including public interest groups, industry and trade associations, and state and local authorities. We reviewed reports and best practices from federal advisory committees, trade associations, and consumer groups. We reviewed our prior recommendations, as well as those made by DHS, the Communications Security, Reliability, and Interoperability Council, and the National Security Telecommunications Advisory Committee related to priority telecommunications services. We also searched various Web-based databases to identify existing articles, peer-reviewed journals, trade and industry articles, government reports, and conference papers.[1] We identified articles from 2010 to 2015. We examined summary-level information about the literature identified in our search that we believed to be germane to our report. It is possible that we may not have identified all of the reports with findings relevant to our objective, and there may be other challenges affecting IP networks during times of crisis that we did not present.

To determine the actions taken by FCC, DHS, and other stakeholders to ensure the reliability of IP communications during times of crisis, we reviewed relevant FCC proceedings, reports, and documents. Specifically, we reviewed FCC proceedings related to technology transitions and ensuring consumer backup power for continuity of

[1]For example, databases we searched included ProQuest, Ei Compendex, Copper Technical Reference Library, SciSearch: A Cited Reference Science Database, and NTIS: National Technical Information Service.

communications, reports on disruptions to communications reports on major disruptions to 911-related communications,[2] and documents related to outage-reporting information. To identify information on the proposed IP transition experiments, we reviewed AT&T and CenturyLink's proposals, stakeholder comments submitted to FCC on these proposals, and other documents related to the experiments. We assessed FCC's efforts to collect data on the effect of the IP transition against criteria established in the federal Standards for Internal Control.[3] We reviewed relevant DHS documents including the 2013 *National Infrastructure Protection Plan*,[4] the 2010 *Communications Sector Specific Plan*,[5] and the *2012 Risk Assessment Report for Communications*.[6] We also reviewed reports and best practices from the Communications Security, Reliability, and Interoperability Council and the Alliance for Telecommunications Industry Solutions.

To obtain additional information on the challenges affecting IP networks and how these challenges affect end users, and to obtain information on state efforts to ensure reliability we selected locations in six states—New York, New Jersey, Arizona, California, Florida, and Alabama—to provide additional details. We selected these locations because they represent a mix of communities that experienced a major communications outage since 2012 or contain an area with a proposed IP transition experiment. These regions also contain a mix of rural, suburban, and urban communities, and demographics including economic differences and average age of residents. We reviewed documents such as reports, comments to FCC, and comments to state agencies. We interviewed officials from state Public Utility Commissions or similar agencies including the New York Department of Public Service, New Jersey Board

[2]FCC, *Impact of the June 2012 Derecho on Communications Networks and Services* (January 2013) and FCC, *April 2014 Multistate 911 Outage: Cause and Impact* (October 2014)

[3]GAO, *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[4]DHS, *National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: 2013).

[5]DHS, *Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington, D.C.: 2010).

[6]DHS, *Risk Assessment Report for Communications* (Washington, D.C.: September 2012).

of Public Utilities, California Public Utilities Commission, and Florida Public Service Commission.[7] We interviewed representatives from other organizations that had experienced the effects of outages or were involved with the proposed IP transition experiments including the City of Flagstaff, the Arizona Telecommunications and Information Council, the Broadband Alliance of Mendocino County, and the Communications Workers of America. We interviewed officials from FCC and DHS and representatives from AT&T, Verizon, and CenturyLink. We also interviewed representatives from selected stakeholder groups including trade and industry associations and consumer and public interest groups, as shown in table 2. We identified stakeholders to interview based on our review of comments filed in FCC's Technology Transitions proceeding, as well as based on recommendations from other organizations we interviewed.

**Table 2: Additional Organizations Interviewed**

| | Organization | Representation |
|---|---|---|
| **Trade and industry associations** | Association of Public-Safety Communications Officials-International (APCO) | Represents public safety communications professionals. |
| | Competitive Communications Association (COMPTEL) | Represents competitive communications service providers and their supplier partners. |
| | Independent Telephone and Telecommunications Alliance (ITTA) | Represents mid-size communications companies. |
| | National Association of Regulatory Utility Commissioners (NARUC) | Represents state public service commissions that regulate utility services. |
| | National Association of State Utility Consumer Advocates (NASUCA) | Represents the interests of utility consumers. |
| | National Cable & Telecommunications Association | Represents U.S. cable industry. |
| | United States Telecom Association (USTelecom) | Represents telecommunications service providers and suppliers, with members ranging from large publically traded communications corporations to small companies and cooperatives. |
| **Consumer groups (or public interest groups)** | Consumer Action | Represents public interest of low- and moderate income, limited English-speaking and other underrepresented consumers. |
| | New America Foundation | Represents the public interest on a variety of issues, including technology and communications networks. |

[7]Officials from the Alabama Public Service Commission and the Arizona Corporation Commission did not respond to our requests for an interview.

| | Organization | Representation |
|---|---|---|
| | Public Knowledge | Represents the public interest on a variety of issues including telecommunications and consumer rights. |
| **Other** | Communications Workers of America | Represents communications workers, including telecommunications. |

Source: GAO and organization information. | GAO-16-167

# Appendix II: Comments from the Federal Communications Commission

Federal Communications Commission
Washington, D.C. 20554

December 08, 2015

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

Dear Mr. Goldstein:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report titled, *Internet Protocol Transition - FCC Should Strengthen Its Data Collection Efforts to Assess the Transition's Effects* ("Draft Report"). We agree with GAO that the Federal Communications Commission (FCC or Commission) has a critical role "in enhancing the cyber and physical security of the communications infrastructure that is essential to national security and public health and safety."[1] Accordingly, the transition from legacy to modern IP-based networks raises important questions for the Commission about how to provide network and service resiliency and reliability assurance to the nation; it is essential that the Commission has sufficient information to make informed decisions. The Commission has in place a comprehensive data strategy, using the Commission's currently available resources and information technology, to oversee the Nation's technology transitions based on our enduring values.[2] This strategy, however, could be strengthened through the provision of additional resources to leverage big data analytics capability. We agree with GAO's implicit recognition that optimal strategic management or oversight of the technology transition would involve robust data analytics ability.

The Commission Has a Strategy for Technology Transitions Oversight

GAO recommends that: "[t]o strengthen FCC's data collection efforts, the Chairman of FCC should develop a strategy to gather additional information on the IP transition to assess the transition's potential effects on public safety and consumers." The report notes the Commission's January 2014 *Technology Transitions Order* and other ongoing Commission efforts but concludes that the Commission has "little information on the effect of the transition."[3] At the outset, in the *Technology Transitions Order*, the Commission identified our focus on "three key technology transitions that significantly affect

[1] *Draft Report* at 1.

[2] *Technology Transitions et al.*, GN Docket No. 13-5 et al., Order, Report and Order and Further Notice of Proposed Rulemaking, Report and Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, 29 FCC Rcd 1433, 1441, para. 23 (2014) (noting the importance that "four enduring values that have always informed communications law – public safety, universal service, competition, and consumer protection" – endure throughout this transition.") (*Technology Transitions Order*).

[3] *Draft Report* at 26.

customers," changes that "are ongoing and will continue for years."[4] The speculative horizon of these multiple transitions makes any attempt to quantify the effects difficult at best. This is unlike the DTV transition, for example, which involved one defined transition with a definitive endpoint. And unlike the DTV transition, which was statutorily-driven, the technology transitions are "market-driven"[5] and "organic processes without a single starting or stopping point."[6]

Today, the Commission uses data and information provided by carriers to monitor and ameliorate any potential negative effects of the transition. All of our efforts with respect to technology transitions are underpinned by work the Commission does on a daily basis in evaluating and processing network change disclosures filed pursuant to section 251(c)(5) of the Communications Act of 1934, as amended (the Act), and discontinuance applications filed pursuant to section 214 of the Act. Through these mechanisms, the Commission ensures that carriers comply with the statute and our rules, including consumer notification and protection requirements, in implementing their network and service transitions.

Indeed, the Commission recently strengthened its rules implementing sections 214 and 251(c)(5), including by enhancing our network change notification process for retirements of copper facilities to ensure that competitive carriers and retail customers receive sufficient time and information to accommodate network transitions and make informed decisions regarding their ongoing service.[7] The Commission also provided clear direction to industry concerning the circumstances in which approval must be sought before removing a service from the marketplace. The Commission will continue to develop additional data requirements if and when necessary to enhance these roles.

Also, the Commission is continuing to evaluate information supplied on the record in the proceedings that produced the *Emerging Wireline Report and Order*. This material, highly germane to the technology transitions, was extensive and informative. For example, we have sought and received substantial input on our proposal to establish specific criteria for the Commission to use in evaluating the adequacy of modern replacements for legacy services in section 214 discontinuance proceedings. Among other things, these proposed standards would take account of a carrier's consumer education and outreach plan in determining whether to allow removal of a legacy service from the marketplace. These criteria could serve to provide certainty to both carriers and consumers and to ensure that critical functionalities are not lost during the transitions. This work is bolstered by the data that the Commission recently received as part of the comprehensive special access data collection and evaluation, which "will enable us to address critical long-term questions about the state of competition for business data connections," an essential element in the technology transitions.[8] In short, while carriers' voluntary experiments can provide useful data – and, for example, the Commission continues to work closely with AT&T on its proposed experiments, to ensure that if AT&T proceeds and the Commission grants approval, useful data is produced – experiments are by no means the sole mean by which the Commission is overseeing technology transitions to ensure the protection of consumers throughout the process.

---

[4] *Technology Transitions Order*, 29 FCC Rcd at 1440, para. 16.

[5] *Id.* at 1435, para. 1.

[6] *Technology Transitions et al.*, GN Docket No. 13-5 et al., Report and Order, Order on Reconsideration, and Further Notice of Proposed Rulemaking, 30 FCC Rcd 9372, 9374, para. 3 (2015) (*Emerging Wireline Report and Order*).

[7] *Id.* at 9375, para. 5.

[8] *Id.* at 9377, para. 6.

Targeted Data Collections are Enabling Public Safety in a Transitioning Environment

The purpose of the GAO Report is to address "the reliability of the nation's communications network in an IP environment during times of crises. . . ."[9] Although the Draft Report focuses on information collected through the Commission's service-based experiments, the Commission has modified several of its information collection initiatives to provide data on the reliability and resiliency of IP-based networks nationwide.[10]

As described in the Draft Report, the Commission's Network Outage Reporting System (NORS) collects detailed information about major disruptions to voice communications on both TDM and IP-based networks.[11] The NORS disruption report data allow the Commission to analyze the reliability of communications infrastructure, and facilitate development of communications industry best practices that have enhanced network resiliency and reliability.[12] Among other continuing developments related to NORS, and in recognition of the critical role undersea cable plays in the nation's global IP-based connectivity and key economic and national security communications, the Commission recently issued a Notice of Proposed Rulemaking to ensure that undersea cable outage data is reported by cable licensees in NORS. This data, would provide further network health assurance in the technology transitions and beyond.[13] These NORS proceedings are ongoing, and reflect the FCC's consideration of the need to extend its network assurance data collection efforts to the IP environment under an appropriate framework.

The GAO Report also observes that the FCC gathers information on the reliability and resiliency of the nation's 911 networks through an annual certification process adopted in 2013.[14] The first such certifications were filed in October 2015 and have provided the FCC with a wealth of information

[9] *Draft Report* at 2.

[10] In addition to its own technology transitions data collection efforts, the Commission also presented to Congress a plan proposing "potential steps for Congress to take to create a legal and regulatory environment that will assist states, PSAPs, service providers and other stakeholders in accelerating the nationwide transition from legacy 911 to NG911." Federal Communications Commission, Legal and Regulatory Framework for Next Generation 911 Services, Report to Congress and Recommendations at § 2 (2013), https://apps.fcc.gov/edocs_public/attachmatch/DOC-319165A1.pdf.

[11] *Draft Report* at 17.

[12] While the foundations of NORS were laid before the current technology transitions, the FCC in 2012 responded to the increasing popularity of interconnected voice over Internet Protocol (VoIP) services by requiring interconnected VoIP providers to report major service disruptions, including disruptions in 911 service. *The Proposed Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers*, Report and Order, 27 FCC Rcd 2650 (2012) (*VoIP Part 4 Order*). In the same proceeding the Commission established a record on broadband network disruption reporting though it has deferred action on that topic. *Id.* at 2651, para. 1. Congress also assigned the Commission a role in promoting IP-911 services. *See* New and Emerging Technologies 911 Improvement Act of 2008 (*NET 911 Improvement Act*), PL 110–283, 122 Stat 2620 (2008). The Commission specifically required interconnected VoIP providers to file plans detailing their compliance with E911 obligations. 47 C.F.R. § 9.5(f).

[13] *See generally VoIP Part 4 Order*, 27 FCC Rcd 2650; *Improving Outage Reporting for Submarine Cables and Enhancing Submarine Cable Outage Data*, Notice of Proposed Rulemaking, 30 FCC Rcd 10492 (2015).

[14] *See Reliability and Continuity of Communications Networks, Including Broadband Technologies*, Report and Order, 28 FCC Rcd 17476 (2013).

regarding the network architectures, backup power strategies,[15] and network monitoring capabilities employed by hundreds of 911 service providers nationwide, representing both urban and rural service areas. Furthermore, the FCC requested comment in 2014 on additional proposals to improve 911 governance and accountability, including a proposal to include topics such as software and database testing and maintenance as part of the 911 reliability certification.[16] Irrespective of any 911 reliability challenges revealed through the service-based experiments, this annual certification process provides the FCC with comprehensive information about the reliability of the nation's 911 networks throughout the technology transitions.

The Commission is also acting to collect technology transitions data in other communications segments that collectively provide the Commission with a greater understanding of the effect of the on public safety. Last year, the Commission revised its questionnaire for the annual 911 Fee Report, regarding the collection and use of state 911 fees, in order to get better information about how states are investing in Next Generation 911.[17] This year's report will be the first time the Commission will analyze this data.[18] In the broadcast segment, the Commission updated the Emergency Alert System (EAS) test system to create the Emergency Test Reporting System (ETRS) database, recognizing that "[o]ur rules governing these alerts must continue to evolve as legacy networks and services transition to next generation technologies."[19] This data source will serve as a "practical, accessible, and minimally burdensome tool for recording EAS dissemination data and developing an FCC Mapbook that can illustrate the manner in which an EAS alert is propagated throughout part or all of the United States."[20]

In the wireless context, the ability to send a text message to 911 in an emergency situation is an obvious benefit of the technology transitions. To support this evolution, and apprise itself of the readiness of the nation's ability to utilize text-to-911 technology, the Commission maintains a Text-to-911 Registry that provides notice of which Public Safety Answering Points (PSAPs) support the text-to-911 function.[21] Wireless technology transitions have also enabled better location accuracy for first responders. This year the Commission issued new standards for wireless location accuracy and is requiring wireless service providers to report on their plans and progress, including the development of

[15] Indeed, the backup power information gathered by the FCC over time has led to the development and adoption of specific rules requiring service providers to make available to their customers certain backup power solutions, and to inform them of those options at points of sale. *See Ensuring Continuity of 911 Communications*, Report and Order, 30 FCC Rcd 8677 (2015). This was driven entirely by the technology transitions awareness gap experienced by consumers in going from traditionally line-powered services to non-line powered services. This is a key example of the way in which the FCC has gathered information on technology transitions and addressed specific consumer needs to ensure continued connectivity and access to public safety services.

[16] *See 911 Governance and Accountability; Improving 911 Reliability*, Policy Statement and Notice of Proposed Rulemaking, 29 FCC Rcd 14208 (2014).

[17] Pursuant to the New and Emerging Technologies 911 Improvement Act, Pub. L. 110-283 (2008).

[18] The report will be out on or before Dec. 31, 2015. The Commission's prior Fee Reports are available at https://www.fcc.gov/encyclopedia/911FeeReports.

[19] *Review of the Emergency Alert System*, Sixth Report and Order, 30 FCC Rcd 6520, 6521, para. 1 (2015).

[20] *Id.* at 6521, para 2.

[21] *See Public Safety and Homeland Security Bureau Announces Update to PSAP Text-to-911 Readiness and Certification Registry*, PS Docket Nos. 10-255, 11-153, Public Notice, 30 FCC Rcd 8196 (PSHSB 2015). The Commission has streamlined this data process so that the Registry of PSAPs capable of receiving Text-to-911 is continuously updated and available via an online database. *Id.*

the National Emergency Address Database that will provide for better indoor location accuracy.[22] Additionally, when the Commission made new spectrum available for Citizens Broadband Radio Service this year, it did so with the requirement that the Spectrum Access System Administrators must take network security into account and provide the security models to the Commission for review.[23]

The Commission has also taken other new approaches to leverage data as technologies evolve and better understand the effects of the technology transitions on public safety. Recognizing the need to respond to dynamic changes in the IP environment, the FCC has actively engaged with the private sector and other relevant stakeholders through mechanisms such as federal advisory committees, including the Communications Security, Reliability, and Interoperability Council (CSRIC) and the Technological Advisory Council (TAC), to better understand the dynamic of the technology transformations.

The Draft Report states that "CSRIC has not specifically looked at ways to improve reliability of IP-networks."[24] I note that CSRIC has been studying IP resiliency issues for years. For example, CSRIC II, which was chartered from 2009-2011, made recommendations on cybersecurity best practices and best practices related to E911 for VoIP services, investigated the transition to an "all-IP NG 911," made recommendations for national security/emergency preparedness priority services in an all-IP environment, and made recommendations on ISP network protection.[25] The Commission received recommendations from CSRIC IV earlier this year on how it can assure that communications sector entities are implementing adequate cyber risk management processes;[26] the Commission is in the process now of evaluating and implementing these recommendations. The Commission has also charged CSRIC with understanding the barriers to cyber threat information sharing among providers in order to better secure IP-based communications services.[27] The Commission's Technical Advisory Committee has been tasked with developing an understanding of the cybersecurity vulnerabilities that accompany increased smart phone usage, a key method of consumer and public safety communications.[28] Finally, the Commission

[22] *Wireless E911 Location Accuracy Requirements*, Fourth Report and Order, 30 FCC Rcd 1259, 1257, para. 37 (2015).

[23] *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 3959, 4061, para. 346 (2015).

[24] *Draft Report* at 18.

[25] *See* FCC Encyclopedia, Communications Security, Reliability and Interoperability Council II, Working Groups, https://www.fcc.gov/pshs/advisory/csric/wg-descriptions.pdf (last visited Nov. 20, 2015).

[26] CSRIC IV, Working Group 4 Final Report, Cybersecurity Risk Management and Best Practices at 1 (Mar. 2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf (last visited Nov. 18, 2015).

[27] *See* CSRIC V Working Group Descriptions and Leadership at 4-5 (charge to Working Group 5) https://transition.fcc.gov/bureaus/pshs/advisory/csric5/Working_GroupCSRICV_110515.pdf (last visited Nov. 18, 2015).

[28] *See* FCC Technological Advisory Council, 2012, Wireless Security & Privacy Working Group presentation (Oct. 31, 2012). *See also* FCC Technological Advisory Council, 2013, Cloud Security Recommendations (Dec. 9, 2013); FCC Technological Advisory Council, 2014, Recommendations on Supporting the Transition to IP, Recommendations for Mobile Device Security and Privacy and Recommendations for Evolution to Internet of Things (Dec. 4, 2014).

has begun analyzing network security plans in the context of mergers and acquisitions in order to protect against security gaps and to ensure network resiliency moving forward.[29]

Additional Resources are Needed to Evolve Data Analysis

As described above, the Commission has executed on numerous aspects of its strategy to collect the data necessary to ensure the core values of communications remain intact throughout the technology transitions. While the data collected offer significant insights into the technology transitions, additional resources would give the Commission the desired holistic data view needed, and thus further the Commission's mission. As Chairman Wheeler recently testified before Congress, the Commission currently lacks the ability to translate its numerous data collection programs into the type of system that would allow for "big data" analytics of the operational status of our nation's networks.[30]

Conclusion

Thank you for the opportunity to respond to the Draft Report. The technology transitions offer a unique opportunity to advance communications services in a manner that maximizes value to the public while minimizing, to the extent feasible, risk to the nation's consumers and businesses. We agree with GAO about the importance of ensuring an informed, data-driven process for determining which services can be seamlessly supported during the transition, which services will need to be transformed, and which services will no longer be supported in an IP world, while preserving the core functions of public safety, universal service, competition, and consumer protection. The Commission's strategy for doing so combines traditional regulatory approaches with innovative methods that match the dynamism of the communications environment, and we are committed to making sure that this strategy is informed by adequate data through our rules, policies, and regular outreach to affected communications industry sectors. The Commission looks forward to working with GAO towards this critical mission.

Sincerely,

David Simpson
Rear Admiral (ret.), USN
Chief, Public Safety and Homeland Security Bureau

[29] *See, e.g.*, Letter from William T. Lake, Chief, Media Bureau, to Catherine Bohigian, Executive Vice President, Gov't Affairs, Charter Communications, Inc., at Enclosure, 22 (Sept. 21, 2015) https://apps.fcc.gov/edocs_public/attachmatch/DOC-335394A2.pdf.

[30] FCC Oversight: Hearing Before the Subcomm. on Commc'n and Tech. of the H. Comm. Energy and Com., 114th Cong. (Nov. 17, 2015) (testimony of FCC Chmn. Tom Wheeler).

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

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

## Staff Acknowledgments

In addition to the individual named above, Sally Moino (Assistant Director), Richard Calhoon, David Hooper, Michael Kaeser, Aaron Kaminsky, Malika Rice, Amy Rosewarne, and Andrew Stavisky made key contributions to this report.

# Related GAO Products

*Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*. GAO-15-714. September 29, 2015.

*Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies*. GAO-15-725T. June 24, 2015.

*Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*. GAO-15-573T. April 22, 2015.

*Information Security: IRS Needs to Continue Improving Controls over Financial and Taxpayer Data*. GAO-15-337. March 19, 2015.

*Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*. GAO-15-221. January 29, 2015.

*Information Security: Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk*. GAO-15-220T. November 18, 2014.

*Information Security: VA Needs to Address Identified Vulnerabilities*. GAO-15-117. November 13, 2014.

*Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*. GAO-15-6. December 12, 2014.

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

## 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

Katherine Siggerud, Managing Director, siggerudk@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