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 Highlights

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

December 2015

INTERNET PROTOCOL TRANSITION

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

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

Tables

Figures

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.