



January 2014

CRITICAL INFRASTRUCTURE PROTECTION

More Comprehensive
Planning Would
Enhance the
Cybersecurity of
Public Safety Entities'
Emerging Technology

GAO Highlights

Highlights of [GAO-14-125](#), a report to congressional requesters

Why GAO Did This Study

Individuals can contact fire, medical, and police first responders in an emergency by dialing 911. To provide effective emergency services, public safety entities such as 911 call centers use technology including databases that identifies phone number and location data of callers. Because these critical systems are becoming more interconnected, they are also increasingly susceptible to cyber-based threats that accompany the use of Internet-based services. This, in turn, could impact the availability of 911 services.

GAO was asked to review federal coordination with state and local governments regarding cybersecurity at public safety entities. The objective was to determine the extent to which federal agencies coordinated with state and local governments regarding cybersecurity efforts at emergency operations centers, public safety answering points, and first responder organizations involved in handling 911 emergency calls. To do so, GAO analyzed relevant plans and reports and interviewed officials at (1) five agencies that were identified based on their roles and responsibilities established in federal law, policy, and plans and (2) selected industry associations and state and local governments.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security collaborate with emergency services sector stakeholders to address the cybersecurity implications of implementing technology initiatives in related plans. DHS concurred with GAO's recommendation.

View [GAO-14-125](#). For more information, contact Gregory C. Wilshusen at 202-512-6244 and wilshuseng@gao.gov

January 2014

CRITICAL INFRASTRUCTURE PROTECTION

More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology

What GAO Found

The five identified federal agencies (Departments of Homeland Security, Commerce, Justice, and Transportation and Federal Communications Commission (FCC)) have to varying degrees, coordinated cybersecurity-related activities with state and local governments. These activities included (1) supporting critical infrastructure protection-related planning, (2) issuing grants, (3) sharing information, (4) providing technical assistance, and (5) regulating and overseeing essential functions. However, except for supporting critical infrastructure planning, federal coordination of these activities was generally not targeted towards or focused on the cybersecurity of state and local public safety entities involved in handling 911 emergency calls.

Under the critical infrastructure protection planning activity, the Department of Homeland Security (DHS) coordinated with state and local governments and other federal stakeholders to complete the *Emergency Services Sector-Specific Plan*. The plan is to guide the sector, including the public safety entities, in setting protective program goals and objectives, identifying assets, assessing risks, prioritizing infrastructure components and programs to enhance risk mitigation, implementing protective programs, measuring program effectiveness, and incorporating research and development of technology initiatives into sector planning efforts. It also addressed aspects of cybersecurity of the current environment. However, the plan did not address the development and implementation of more interconnected, Internet-based planned information technologies, such as the next generation of 911 services. According to DHS officials, the plan did not address these technologies, in part, because the process for updating the sector-specific plan will begin after the release of the revised National Infrastructure Protection Plan—a unifying framework to enhance the safety of the nation's critical infrastructure. A revised plan was released in December 2013, and, according to DHS, a new sector-specific plan is estimated to be completed in December 2014. Until DHS, in collaboration with stakeholders, addresses the cybersecurity implications of the emerging technologies in planning activities, information systems are at an increased risk of failure or being unavailable at critical moments.

Under the other four activities, federal agencies performed some coordination related activities for public safety entities including administering grants for information technology enhancements, sharing information about cyber-based attacks, and providing technical assistance through education and awareness efforts. For example, the Departments of Transportation and Commerce allocated \$43.5 million in grants to states over a 3-year period, starting in September 2009, to help implement enhancements to 911 system functionality. While these grants were not targeted towards the cybersecurity of these systems, cybersecurity was not precluded from the allowed use of the funds.

Contents

Letter		1
	Background	2
	Identified Federal Agencies Have Had Limited Coordination with State and Local Governments Regarding Cybersecurity at Public Safety Entities	16
	Conclusions	24
	Recommendation	24
	Agency Comments and Our Evaluation	25
Appendix I	Objective, Scope, and Methodology	28
Appendix II	Comments from the Department of Homeland Security	31
Appendix III	Comments from the Federal Communications Commission	34
Appendix IV	GAO Contact and Staff Acknowledgments	36
Tables		
	Table 1: Sources of Cybersecurity Threats	8
	Table 2: Types of Exploits	9
Figure		
	Figure 1: Overview of Public Safety Communications and Dispatch System	4

Abbreviations

DHS	Department of Homeland Security
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
NG 911	Next Generation 911
NIPP	National Infrastructure Protection Plan
NTIA	National Telecommunications and Information Administration
PSAP	Public Safety Answering Point
VoIP	Voice over Internet Protocol

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



January 28, 2014

Congressional Requesters

In an emergency, individuals can contact fire, medical, and police first responders by dialing 911. Across the nation, millions of emergency calls are made annually to public safety entities that dispatch first responders to the scene. To provide these emergency services, public safety entities use information technology that includes databases with geographic, phone number, and location data.¹ These technologies increasingly rely on the Internet, which makes them susceptible to cyber-based threats that could impact the availability of 911 services. Since 2003, we have identified the protection of systems supporting our nation's critical infrastructure (which includes the emergency services sector²) as a governmentwide high-risk area, and we continued to do so in the most recent update to our high-risk list.³

At your request, we reviewed federal coordination with state and local governments regarding cybersecurity at public safety entities. Our objective was to determine the extent to which federal agencies

¹As used in this report, the term "public safety entities" refers to the organizations responsible for accepting and responding to emergency calls. They include the various levels of help required to respond to an emergency, such as the public safety answering point (a 911 call center or its equivalent) that accepts the emergency call, assists the caller, and sends the appropriate first responder(s) to the caller's location. First responder organizations include law enforcement, fire and rescue, and emergency medical services sent to assist the caller. An emergency operations center is typically established to address a specific environmental emergency (such as a hurricane, severe snowstorm, or forest fire), a special event, man-made disaster, or when such an environmental threat is imminent.

²The emergency services sector is 1 of 16 critical infrastructure sectors established by federal policy. The other sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

³GAO's biennial High-Risk List identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need to address challenges to economy, efficiency, or effectiveness. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our nation's critical infrastructure. See GAO, *High-Risk Series: An Update*, [GAO-13-283](#) (Washington, D.C.: February 2013).

coordinate with state and local governments regarding cybersecurity efforts at emergency operation centers, public safety answering points (PSAP), and first responder organizations involved in handling emergency calls.

To conduct our evaluation, we analyzed federal law, policy, and plans to identify key federal agencies and their responsibilities for coordinating and assisting state and local governments with their cybersecurity efforts. Based on this analysis, we identified five agencies (the Departments of Homeland Security, Commerce, Justice, and Transportation and the Federal Communications Commission) for review. We focused on the following five coordination-related activities: (1) supporting critical infrastructure protection-related planning, (2) issuing grants, (3) sharing information, (4) providing technical assistance, and (5) regulating and overseeing essential functions. For each identified agency, we collected and analyzed relevant plans and reports dated from 2010 to 2013, and interviewed officials to determine the extent to which each agency had performed these activities with state and local governments relative to the cybersecurity efforts at public safety entities involved in 911 emergency calls. To confirm federal efforts and gain an understanding regarding how public safety entities operate, we analyzed relevant policies, plans, and reports and interviewed officials familiar with emergency operations and/or cybersecurity aspects of state and local governments from seven industry associations. We also interviewed officials familiar with emergency communication operations based on proximity of location, leadership in national associations, and/or involvement in ongoing technology enhancements from seven state and local governments relevant to public safety operations.

We conducted this performance audit from November 2012 to January 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Appendix I contains additional details on the objective, scope, and methodology of our review.

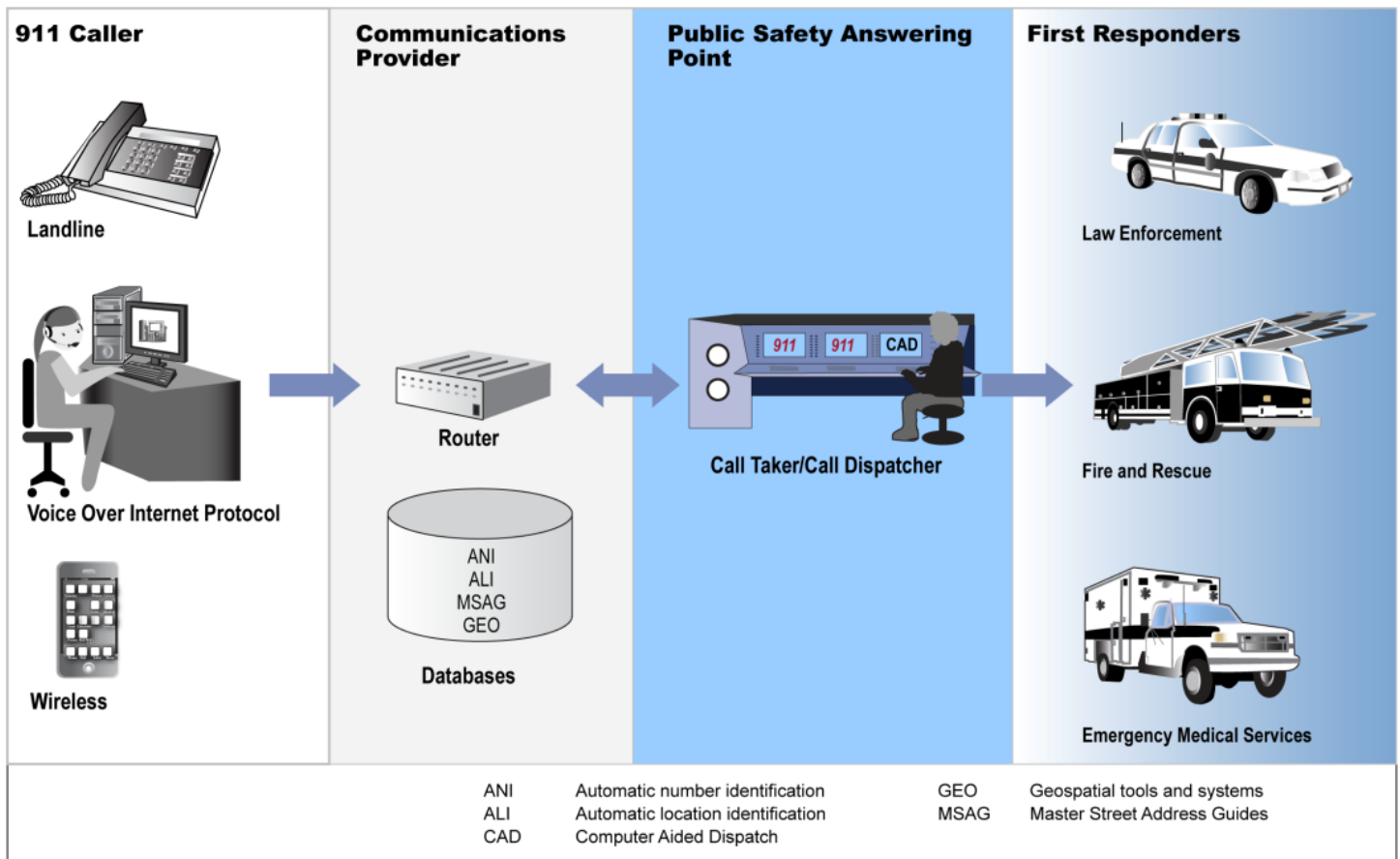
Background

The 911 emergency call system is intended to give individuals a simple, easy-to-remember, routinely available number that can be used to reach an appropriate public safety provider during any life-threatening situation. Using a landline, wireless, mobile telephone, or voice over internet

protocol (VoIP) system, a caller dials 911 and the call is routed to a communications provider facility that automatically forwards the call to a public safety entity such as a PSAP. Next, the call taker/dispatcher talks to the caller to determine the nature of the emergency and to determine the necessary first responders, while working to send (or dispatch) the appropriate first responders to the location. According to the National Emergency Number Association,⁴ there are more than 6,000 PSAPs nationwide, at a county or city level, that answer more than 240 million 911 calls each year. Figure 1 illustrates the public safety communications and dispatch system, including how an emergency call is typically placed, received, and processed.

⁴The National Emergency Number Association is a nonprofit, professional organization that is focused on 911 policy, standards development, technology, operations, and education issues. It has more than 7,000 members from the public safety and 911 industries.

Figure 1: Overview of Public Safety Communications and Dispatch System



Source: Based on GAO analysis of public safety industry documents.

As illustrated in figure 1, once a 911 caller places an emergency call, the communications provider receives and routes the call to the appropriate PSAP. The system used to route the call depends on the type of telephone used to make the 911 call. Specifically, for a call placed from a landline, a router in the provider’s central facility receives the 911 call and accesses the Automatic Number Identification database to associate the identifier with the phone number to determine the caller’s address. Then, based on the location information, the provider’s Master Street Address Guide database identifies the appropriate PSAP to receive the call. When a cell phone is used, the location information is typically provided to the PSAP through either cell tower triangulation technology or by Global Positioning System technology. When using VoIP, where calls are carried over digital subscriber lines, cable modems, or other Internet access

methods, the caller needs to register the address of the VoIP device in advance. Current telecommunications and PSAP technology associate the voice and data transmission with the identifier and location databases and, based on the caller's location, routes the call to the appropriate PSAP.

When the caller's phone number, address, and voice are routed to the appropriate PSAP, the call is automatically delivered with the phone number and location. The trained 911 call taker/dispatcher assists the caller and inputs information into additional IT systems and infrastructure to begin the emergency response. For example, the call taker/dispatcher may enter information into a computer-aided dispatch system. These systems automate the call-taking process, provide questions and responses for various scenarios, and send the first responders. Based on the information put into the system by the call taker/dispatcher, the computer-aided dispatch system interfaces with other systems for identification and address, ascertains the nature of the assistance needed, and transmits the information to the appropriate first responder. To provide assistance to the first responder, the call taker/dispatcher may also be able to use geospatial tools and systems that provide information on utility placement, government facility types and locations, property plats, mapping data, and aerial photographs. In addition, call takers may use criminal justice information databases, Internet access, automated vehicle locators to select the closest first responder, and radio and telecommunications services to share and receive information as the situation warrants.

While a PSAP is to be available on a 24-hours, 365 day-a-year basis, an emergency operations center, as noted, is typically only activated during an environmental emergency or special event. It provides a single location for key decision makers from state, local, and federal agencies and multiple jurisdictions to gather and to react to events too complex or too large for regular offices or communications centers or single government agencies or jurisdictions to handle. From a single location, the officials can support on-scene incident commanders (such as fire, police, and emergency medical personnel), prioritize the allocation of resources, collaborate on strategy and tactics, and manage the fiscal and social consequences of an incident.

Emergency operations centers require the same variety of information and communications technology used by PSAPs to fulfill their mission: Internet access, telecommunications services, geospatial tools, and radio systems. In addition, these centers have access to and use public alerting

and warning systems to disperse information to citizens, such as sending messages to registered devices (mobile telephones, pagers, electronic mail, etc.), sirens, public address systems, and, in some cases, reverse 911 or similar products that can send warnings to entire communities when the need arises.

Next Generation of Public Safety Communications Will Be Even More Reliant on IT

Public safety entities are undergoing the process of implementing the next generation of 911 services (known as NG 911) to, among other things, improve their capabilities to communicate with callers, increase resiliency of their 911 operations, and enhance information sharing among first responders. NG 911 is expected to use Internet protocol-based, broadband technology that is capable of carrying voice plus large amounts of varying types of data, such as instant messaging, wireline calls, VoIP calls, photographs, live video feeds from an emergency scene, and “telematics” (such as advanced automatic crash notification data collected from the vehicle’s computer system).⁵ Some states have implemented NG 911 functionality in selected PSAPs in order to ascertain technology requirements and cybersecurity implications with the intention of using multiple releases to eventually move to full NG 911 capability. For example, in 2011, California began conducting multiple pilots to evaluate different technology platforms for its NG 911 operations such as hosted or cloud-based technology.⁶ In 2012, Vermont completed a 6-month pilot accepting text messages in lieu of voice 911 calls from a wireless carrier. Vermont has also implemented a statewide 911 system that transmits 911 calls to PSAPs using VoIP for its emergency services network.

In addition, the Middle Class Tax Relief and Job Creation Act of 2012⁷ required the National Telecommunications and Information Administration

⁵Telematics is the integration of information and communications technology to send, receive, and store information. Telematics in vehicles includes emergency warning systems, global positioning systems, and integrated hands-free cell phones.

⁶According to the National Institute of Standards and Technology, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. National Institute of Science and Technology, *The NIST Definition of Cloud Computing*, SP 800-145, (Gaithersburg, Md.: September 2011).

⁷Pub. L. No. 112–96 (Feb. 22, 2012).

(NTIA) and Transportation's National Highway Traffic Safety Administration to create a program to improve emergency communications throughout the country by facilitating coordination and communication among federal, state, and local emergency communications systems, emergency personnel, public safety organizations, telecommunications providers, and telecommunications equipment manufacturers and vendors involved in the implementation of 911 services. The act established FirstNet as an independent authority within the NTIA to develop a single nationwide, interoperable public safety broadband network. The FirstNet network is intended to give users functionality beyond current radio communications such as access to video images of a crime in progress, downloaded floor plans of a burning building, and rapid connection with first responders from other communities. The network is expected to be IP-based and interface with commercial networks to transmit voice, text, photographic, video, and other digital data between PSAPs and first responders using interoperable mobile devices and leveraging NG 911 technology.

As of October 2013, the FirstNet network requirements had not been developed; however, the Middle Class Tax Relief and Job Creation Act of 2012 required functionality to include public Internet connectivity over commercial wireless networks or the public switched telephone network. The act also required that FirstNet's network development ensure the safety, security, and resiliency of the network, including requirements for protecting and monitoring the network to defend against cyberattack. The act does not specify time frames for completing implementation of the network.

Threats to Public Safety Cyber Infrastructure

Like threats affecting other critical infrastructures, threats to the public safety IT infrastructure can come from a wide array of sources. For example, advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risk. Other sources include corrupt employees, criminal groups, hackers, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary or political gain or mischief, among other things. Table 1 describes the sources of cyber-based threats in more detail.

Table 1: Sources of Cybersecurity Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Insiders	A disgruntled or corrupt organization insider is a source of computer crime. The insider may not need a great deal of knowledge about computer intrusions because his or her knowledge of a target system is sufficient to allow unrestricted access to cause damage to the system or to steal system data. The insider threat includes malicious current and former employees and contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. A phisher may also use spam and spyware or malware to accomplish objectives.
Spammers	An individual or organization that distributes unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	An individual or organization with malicious intent carries out attacks against users by producing and distributing spyware and malware. Several notable destructive computer viruses and worms have harmed files and hard drives, and caused physical damage to equipment, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, Blaster, and Stuxnet.
Terrorists	A terrorist seeks to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. The terrorist may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and the Software Engineering Institute's CERT® Coordination Center.

These sources of cyber threats may make use of various cyber techniques, or exploits, to adversely affect communications networks, and could negatively impact Internet-protocol based NG 911 and FirstNet networks. Types of exploits include denial-of-service attacks, phishing, passive wiretapping, Trojan horses, viruses, worms, and attacks on the IT supply chains that support the communications networks. Table 2 describes the types of exploits in more detail.

Table 2: Types of Exploits

Type of exploit	Description
Denial of service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial of service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is performed without altering or affecting the data.
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use an e-mail program to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread. Unlike a computer virus, a worm does not require human involvement to propagate.
Exploits affecting the IT supply chain	The installation of hardware or software that contains malicious logic (like a logic bomb, Trojan horse, or a virus) or an unintentional vulnerability (the result of an existing defect, such as a coding error) or that may be counterfeited. A supply chain threat can also come from the failure or disruption in the production of critical product, or a reliance on a malicious or unqualified service provider for the performance of technical services.

Source: GAO analysis of unclassified governmental and nongovernmental data.

In addition to cyber-based threats, the nation's public safety entities also face threats from physical sources. Examples of these threats include natural events (e.g., hurricanes or flooding) and man-made disasters (e.g., terrorist attacks), as well as unintentional man-made outages (e.g., a backhoe cutting a communication line). For example, after a major storm in June 2012, several cities and counties in Virginia experienced a total outage of telephone service supporting 911 that continued for 5 days. The loss of commercial power and the subsequent failure of one of the two backup generators in the common carrier's facilities were the predominant causes of the service outage. In addition, the lack of physical diversity in the telephone circuits supporting 911 and the failure to monitor the telephone circuits contributed to the disruption of PSAP operations during the outage.⁸

⁸ FCC, Impact of the June 2012 Derecho on Communications Networks and Services (Washington, D.C.: January 2013).

While not related to public safety entities' internal IT, these organizations, specifically PSAPs, have been the target of attacks and pranks. For example, in March 2013, the National Emergency Number Association reported that more than 200 telephony-based attacks had been identified.⁹ The attacks were part of an extortion scheme demanding payment for an outstanding debt to be paid to an individual or organization. When the request was not paid, the perpetrator launched an attack that inundated the PSAP's administrative, nonemergency lines with a continuous stream of calls for a lengthy period of time.

In addition, PSAPs have received false emergency calls from pranksters who use Internet protocol-based telephone technology to camouflage the source of the call. In these cases, a caller reported a serious incident in progress, such as an armed robbery or a home invasion, and a false address or location information make it appear that the call is coming from a different address. For example, in April 2013, news media reported that multiple celebrities' homes were swarmed by police after fake 911 calls were made reporting a crime in progress involving people armed with guns or bombs.¹⁰ The incidents occupied public safety resources that otherwise could have been available to receive and respond to actual emergency calls.

Identified Federal Agencies Are to Support and Coordinate with State and Local Governments Regarding Cybersecurity Efforts

Although state and local governments are responsible for the operation and cybersecurity of their public safety entities, federal law, policy, and plans specify roles and responsibilities for the Departments of Homeland Security, Commerce, Transportation, and Justice and the Federal Communications Commission to support state and local governments' cybersecurity efforts. These agencies are responsible for performing one or more of the following cybersecurity-related coordination roles and responsibilities: (1) supporting critical infrastructure protection-related

⁹National Emergency Number Association, *Telephony Denial of Services (TDoS) to Public Safety Communications Phone Service: Recommended Best Practices Checklist* (Alexandria, Va: March 22, 2013).

¹⁰William Jackson, "Phone-DOS attacks in extortion scam target gov offices," *Government Computer News*, Apr. 3, 2013, <http://gcn.com/articles/2013/04/03/phonedos-attacks-extortion-scam-target-gov-offices.aspx>, accessed November 25, 2013 and Brian Prince, "DHS, FBI Warn of Denial-of-Service Attacks on Emergency Telephone Systems," *eWEEK*, Apr. 3, 2013 <http://www.eweek.com/security/dhs-fbi-warn-of-denial-of-service-attacks-on-emergency-telephone-systems/>, accessed November 25, 2013.

Department of Homeland Security

planning, (2) issuing grants, (3) sharing information, (4) providing technical assistance, and (5) regulating and overseeing essential functions.

DHS is responsible for leading, integrating, and coordinating the implementation of efforts to protect the nation's cyber-reliant critical infrastructures. The Homeland Security Act of 2002 created DHS and, among other things, assigned it the following critical infrastructure protection responsibilities: (1) developing a comprehensive national plan for securing the critical infrastructures of the United States, (2) recommending measures to protect those critical infrastructures in coordination with other groups, and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of, or response to, terrorist attacks.¹¹ In addition, under the act, DHS is required to provide to state and local government entities analysis and warnings related to threats and vulnerabilities to their critical information systems, crisis management support in response to threats or attacks, and technical assistance with emergency recovery plans for critical information systems.

In 2003, Homeland Security Presidential Directive 7 (HSPD-7)¹² established DHS as the principal federal agency to lead, integrate, and coordinate the implementation of efforts to protect cyber-critical infrastructures and key resources. In addition, HSPD-7 identified lead federal agencies, referred to as sector-specific agencies, that are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors.

In 2009, in accordance with the Homeland Security Act, DHS issued the National Infrastructure Protection Plan (NIPP).¹³ The plan sets forth a risk management framework and details the roles and responsibilities of DHS in protecting the nation's critical infrastructures; identifies agencies with

¹¹Pub. L. No. 107-296 (Nov. 25, 2002).

¹²The White House, *Homeland Security Presidential Directive 7* (Washington, D.C.: Dec. 17, 2003).

¹³DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009). This plan is to provide the unifying structure for the integration of existing and future critical infrastructure and key resource protection efforts and resiliency strategies into a single national program to achieve this goal.

lead responsibility for coordinating with the sectors (or sector-specific agencies); and specifies how other federal, state, regional, local, tribal, territorial, and private-sector stakeholders should use risk management principles to prioritize protection activities within and across sectors. As the sector-specific agency for the emergency services sector, DHS is to coordinate protective programs and resilience strategies for the sector. The emergency services sector is comprised of assets, systems, and networks supporting law enforcement, fire and emergency services, emergency management, emergency medical services, and public works functions at the state, local, tribal, and territorial levels of government.

Based on NIPP, DHS is tasked with, among other things, updating the sector-specific plans, coordinating sector training, and maintaining information-sharing mechanisms. DHS is to collaborate with public- and private-sector stakeholders through government and sector coordinating councils to develop and implement the sector-specific plan in order to identify and protect critical infrastructure assets.¹⁴ In addition, DHS is responsible for the state, local, tribal, and territorial cybersecurity engagement program, which was established to build partnerships with non-federal public stakeholders including governors, mayors, state homeland security advisors, chief information officers, and chief information security officers, in order to advance the department's mission in protecting critical network systems and ensuring the use of the Internet as a resource to connect with citizens.

In February 2013, Presidential Policy Directive 21 directed the Secretary of Homeland Security to update NIPP by October 2013. However, it states that all plans remain in effect until specifically revoked or superseded. It also revoked HSPD-7 but continued to identify DHS as the

¹⁴Sector-specific planning and coordination are addressed through coordinating councils that are established for each sector. Sector Coordinating Councils are comprised of representatives of critical infrastructure owners and operators, generally from the private sector. Government Coordinating Councils are composed of representatives of the sector-specific agencies; other federal departments and agencies; and state, local, tribal, and territorial governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to critical infrastructure protection and work together to advance capabilities.

sector-specific agency for the emergency services sector.¹⁵ The directive also identified sector-specific agency roles and responsibilities for their respective sectors to include (1) coordinating with federal agencies and collaborating with state, local, territorial, and tribal entities; (2) serving as a day-to-day federal interface for the prioritization and coordination of activities; (3) carrying out, consistent with law and policy, incident management; and (4) supporting sector identification of vulnerabilities. DHS released an updated NIPP in December 2013.¹⁶

Department of Commerce

Federal law and policy also establish a role for Commerce in protecting the nation's communications networks. For example, the Telecommunications Authorization Act of 1992 established Commerce's National Telecommunications and Information Administration (NTIA) as the principal presidential adviser on telecommunications and information policies.¹⁷ NTIA activities include administering grant programs that further the deployment and use of broadband and other technologies, and developing policy on issues related to the Internet economy, including cybersecurity.

In addition, as discussed previously, the Middle Class Tax Relief and Job Creation Act of 2012 required NTIA and Transportation's National Highway Traffic Safety Administration to create a program to improve emergency communications throughout the country. The act established FirstNet as an independent authority within the NTIA to develop a single nationwide, interoperable public safety broadband network. FirstNet's responsibilities include leading the development actions including obtaining grants and funds from and making contracts with, among others, private companies and federal, state, regional, and local agencies. In addition, FirstNet is also to ensure the safety, security, and resiliency of the FirstNet network, including requirements for protecting and monitoring the network to protect against cyber attack.

¹⁵The White House, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). This directive revoked Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, issued December 17, 2003.

¹⁶ DHS, *National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

¹⁷Pub. L. No. 102-538 (Oct. 27, 1992); 47 U.S.C. § 902.

Department of Transportation

Based on provisions in the ENHANCE 911 Act of 2004 and Middle Class Tax Relief and Job Creation Act of 2012, Transportation, through the National Highway Traffic Safety Administration, coordinates 911 services at the federal, state, and local levels.¹⁸ Specifically, Transportation operates a program to facilitate coordination and communication between federal, state, and local emergency communications systems, emergency personnel, public safety organizations, telecommunications carriers, and telecommunications equipment manufacturers and vendors involved in the implementation of 911 services. Coordination activities include resources and technical assistance provided to state and local 911 authorities, such as grants supporting upgrades to PSAP equipment and operations and education about implementing new 911 technologies.

Department of Justice

The Federal Bureau of Investigation (FBI), under Justice, leads the nation's efforts in investigating cyber-based crimes including computer intrusions and major cyber fraud. The FBI shares cyber-related information with state and local governments that could be law enforcement sensitive or classified. In particular, the FBI's National White Collar Crime Center in partnership with the Internet Crime Complaint Center is to receive Internet-related criminal complaints; research, develop, and refer the criminal complaints to federal, state, local, and international law enforcement; and issue alerts to affected entities.¹⁹

Federal Communications Commission

The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite, and cable throughout the United States.²⁰ Agency 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, it has the authority to adopt, administer, and enforce rules related to cybersecurity, communications reliability, and 911 and emergency alerting. Its regulations include requirements for certain communications providers to report on the reliability and security of

¹⁸Pub. L. No. 108-494 (Dec. 23, 2004); 47 U.S.C. § 942.

¹⁹The mission of the National White Collar Crime Center is to provide training, investigation support services, and research to agencies and entities involved in the prevention, investigation, and prosecution of economic and high-tech crimes.

²⁰FCC's major statutory authority is the *Communications Act of 1934*, as amended, including by the *Telecommunications Act of 1996*, Pub. L. No. 104-104, 47 U.S.C. Section 151.

communications infrastructures. These include requirements for reporting service disruptions and outages.²¹ For example, communications providers are required to report service outages and related issues that meet specific thresholds that affect public safety communications and emergency response.

Also, the FCC engages in public-private partnerships through federal advisory committees such as its Communications, Security, Reliability, and Interoperability Council. The Council develops and provides recommendations to the FCC regarding best practices and actions that can be taken to ensure optimal security, reliability, and interoperability of commercial and public safety communications systems. Among other efforts, the Council's working group is responsible for assessing and making recommendations concerning technical standards, related technical gaps, and overall readiness of the legacy 911 system for accepting information generated by NG 911 applications. Working group members include representatives from federal, state, and local governments, the telecommunications industry, and industry associations.

In addition, the FCC is required by the Middle Class Tax Relief and Job Creation Act of 2012 to reallocate spectrum for use by public safety entities and to grant a license for that spectrum to FirstNet. Under the act, the FCC is required to establish an advisory board to develop recommended technical requirements to ensure a nationwide level of interoperability for the network. The board is to be known as the "Technical Advisory Board for First Responder Interoperability."²² FCC is also required, in coordination with DHS and the National Highway Transportation Safety Administration, to make recommendations to Congress regarding the legal and statutory framework for NG 911 services to include security standards.

Presidential Policy Directive 21 requires that the FCC is to exercise its authority and expertise to partner with DHS, as well as other federal

²¹ According to FCC regulations, an outage is defined as a significant degradation in the ability of an end user to establish and maintain a channel of communication as a result of failure or degradation in the performance of a communications provider's network.

²² In May 2012, the Technical Advisory Board for First Responder Interoperability issued a report of minimum technical requirements that included recommendations for equipment and device management, testing, and cybersecurity, among other things. Following the issuance of the report, the board was disbanded.

departments and agencies, to: (1) identify and prioritize communications infrastructure; (2) identify communications sector vulnerabilities and work with industry and other stakeholders to address those vulnerabilities; and (3) work with stakeholders, including industry, and engage foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitate the development and implementation of best practices promoting the security and resilience of critical communications infrastructure.

Identified Federal Agencies Have Had Limited Coordination with State and Local Governments Regarding Cybersecurity at Public Safety Entities

The five identified federal agencies have, to varying degrees, coordinated cybersecurity-related activities with state and local governments. Agencies' activities include (1) supporting critical infrastructure protection-related planning, (2) issuing grants, (3) sharing information, (4) providing technical assistance, and (5) regulating and overseeing essential functions. However, except for supporting critical infrastructure planning, federal activities were generally not targeted towards or focused on public safety entities. For example, DHS collaborated with state and local governments through the Sector Coordinating Council to complete critical infrastructure planning efforts. Regarding grants to enhance emergency services, sharing cybersecurity-related information, providing technical assistance, and regulating and overseeing essential functions, federal agencies' coordination activities with state and local governments were generally not targeted to public safety entities' cybersecurity. However, federal agencies performed some coordination-related activities directed to public safety entities, including issuing alerts about cyber-based attacks to public safety entities, performing risk assessments, providing technical assistance through education and awareness efforts, and administering grants that allowed for expenditures for IT equipment and cybersecurity tools.

DHS's Critical Infrastructure Protection Planning Activities Address Cyber Risks in the Current Environment but Do Not Consider Planned Technology Initiatives

In accordance with NIPP, DHS coordinated with state and local governments through the Emergency Service Sector Coordinating Council to develop a draft plan to address the protection of emergency services sector critical infrastructure and key resources. During the process, DHS solicited and obtained input from federal and nonfederal stakeholders through the established government and sector coordinating councils. For example, FCC officials from the Public Safety and Homeland Security Bureau stated that they had coordinated with DHS and other federal entities in the development of the plan. In 2010, DHS issued the Emergency Services Sector-Specific Plan, which addresses, among other things, the cybersecurity of public safety entities such as

PSAPs, emergency operations centers, and first responder agencies. The Emergency Services Sector Coordinating Council acknowledged within the plan that they had provided input during the development process and would work with the various partners to support implementation of the plan.

The Emergency Services Sector-Specific Plan identifies activities that the sector can take to mitigate the overall risk to key assets, systems, networks, or functions, and mitigate vulnerabilities or minimize the consequences associated with a terrorist attack or other incident. The Emergency Services Sector-Specific Plan lists protective programs and resilience strategies for the human, physical, and cyber-critical infrastructure supporting the sector that are available to members of the emergency services sector to assist them in protecting their critical assets. The cyber-related protective programs include homeland security grants, the cross-sector cybersecurity working group, and cyber exercises. The plan is intended to serve as a guide for the sector, including the public safety entities, to set protective program goals and objectives, identify assets, assess risks, prioritize infrastructure components and programs to enhance risk mitigation, implement protective programs, measure program effectiveness, and incorporate research and development of technology initiatives into sector planning efforts. For example, it states that the sector must be able to determine the hardware and software components critical to supporting the sector's mission, including the computers, databases, and other IT assets. Further, DHS, through the plan, recognized the risk of cyber attack on PSAP systems, such as attacks on computer-aided dispatch systems and how such attacks would seriously impede the sector's ability to react and respond swiftly to incidents.

In addition, the NIPP and the Emergency Services Sector-Specific Plan identified the need to assess risks to the sector. In 2012, DHS, based on a collaborative effort with state and local entities and the private sector, issued the Emergency Services Sector Cyber Risk Assessment, which documents DHS and sector subject matter experts' evaluation of the threats, vulnerabilities, and consequences to the sector's cyber infrastructure.²³ The assessment identified intentional and unintentional

²³DHS, *Emergency Services Sector Cyber Risk Assessment* (Washington, D.C.: April 2012).

threats including cyber-related threats that could disrupt or degrade a PSAP's 911 service capabilities. For example, a cyber-related threat could target a computer-aided dispatch system or geospatial database, thus compromising the availability of geographical information and other technical support and reducing the effectiveness of the emergency response. The risk assessment also stated that vulnerabilities to the common carriers' address and location databases are the responsibility of the common carriers and are not within the control of a PSAP. It further stated that the next step is to determine how identified risks should be addressed and will require continued public- and private-sector collaboration. Also, according to the risk assessment, the sector is to develop a strategy for mitigating risks throughout the sector. According to DHS officials responsible for emergency services sector activities, the strategy is scheduled for completion and approval by the end of the second quarter of fiscal year 2014.

While DHS and the Emergency Services Sector Coordinating Council addressed in the 2010 Emergency Services Sector-Specific Plan aspects of cybersecurity of the current environment, they did not address the development and implementation of NG 911 and the FirstNet network in public safety entities. According to the NIPP, sector-specific plans are to identify activities to mitigate overall risk to the key assets, systems, networks, or functions, and mitigate vulnerabilities or minimize the consequences associated with a terrorist attack or other incident. As the sector-specific agency, DHS is tasked with developing and updating the sector-specific plans in coordination with public and private sector stakeholders through government and sector coordinating councils.

However, DHS and the coordinating councils had not yet incorporated cybersecurity protections for NG 911 and the FirstNet network into the sector plan in part because the revision cycle had not occurred and FirstNet was not established until 2012. According to DHS officials, the process for updating the sector-specific plans will begin after the revised NIPP has been released. A revised NIPP was released in December 2013, and, according to DHS, a new sector-specific plan is estimated to be completed in December 2014. Until DHS, in collaboration with stakeholders, develops the next iteration of the sector-specific plan, it is unclear if the cybersecurity implications of implementing these technologies will be considered. Comprehensive planning based on effective coordination between federal and non-federal emergency services sector stakeholders could better position the sector to identify and mitigate the increased cyber-based risks of the NG 911 and FirstNet

network technologies. Without such planning, information systems are at an increased risk of failure or being unavailable at critical moments.

Although Identified Federal Agencies Provided Grants to State and Local Governments, These Grants Did Not Specifically Target Cybersecurity of Public Safety Entities

Federal grant programs have been used to fund technology enhancements so that public safety entities could address the evolution in communications technology and for technology enhancements at state and local public safety entities to include allocations for cybersecurity enhancements at the grantee's option. The National Highway Traffic Safety Administration and the NTIA allocated \$43.5 million in grants to states over a 3-year period, starting in September 2009, to help implement enhancements to 911 system functionality to address the increase in 911 calls from cell phones and the future plans for PSAPs to handle text and other message formats. Eligible expenses under the grant requirements fell into four categories: administrative expenses, training, consulting, and hardware and software. The grant period concluded at the end of fiscal year 2012. In all, the National Highway Traffic Safety Administration and NTIA awarded grants ranging from \$200,000 to \$5.4 million to 30 states and territories to help implement 911 system enhancements. While cybersecurity was not specified as a requirement in a grant program's eligible use of funds, it was not precluded from the allowed use of the funds. In March 2013, the National Highway Traffic Safety Administration and NTIA reported that state governments used the majority of the funds to procure hardware and software to develop the IP-based infrastructure in preparation for their eventual migration to the NG 911 environment.

DHS's Federal Emergency Management Agency (FEMA) offered preparedness program funds to state and local governments in order to enhance their emergency response capabilities. Although FEMA does not have a specific grant program for cyber-related purchases, cybersecurity and IT equipment (i.e., personal and network firewalls, authentication devices, and intrusion detection systems) are among the allowable equipment listed under these grants. The grants also allow for purchases of PSAP-related IT, such as computer-aided dispatch systems, global positioning systems, and automatic vehicle locating systems. According to FEMA officials, the grant money is typically distributed to state governments that, in turn, allocate the funds to local governments for their public safety entities and for other local government operations.

Justice, through its Office of Justice Programs, provided grants to local governments to support cyber forensics, cyber crime investigations, and related training. Justice reported that fiscal year 2012 grants funded

computer equipment purchases, training for law enforcement personnel, and cyber crime awareness and prevention programs. However, based on our analysis of cyber-related grant information provided by Justice officials, the grants were not used for cybersecurity within the local public safety organizations. Local governments used the grants to enhance their capabilities to perform cyber forensics and cyber crime investigations.

At the time of our review, NTIA officials involved in the FirstNet network's implementation stated that NTIA had distributed grants totaling \$122 million to state and local governments for planning and conducting studies to determine the infrastructure, equipment, and architecture requirements for FirstNet's network development.

FCC officials did not identify grant programs that directly or indirectly target improving the security of the networks and computer systems at state and local public safety entities.

DHS and FBI Shared Cybersecurity Information that Could be Relevant to Public Safety Entities' Cybersecurity

DHS shared cybersecurity-related information such as threats and hazards with state and local governments through various entities. While the information was not uniquely targeted to public safety entities, it may be of benefit to them. Specifically,

- DHS collected, analyzed, and disseminated cyber threat and cybersecurity-related information to state and local governments through its National Cybersecurity and Communications Integration Center and through its relationship with the Multi-State Information Sharing and Analysis Center.
- DHS's State, Local, Tribal, and Territorial Engagement Office's Security Clearance Initiative facilitates the granting of security clearances to state chief information officers and chief information security officers. The clearances allow these personnel to receive information about current and recent cyber attacks and threats. For example, according to DHS officials, they have issued secret clearances to 48 percent of state chief information officers and 84 percent of state chief information security officers.
- DHS provides intelligence information to fusion centers, which then share the information on possible terrorism and other threats and

issue alerts to state and local governments.²⁴ For example, in March 2013, a fusion center issued a situational awareness bulletin specific to public safety entities. The alert was about possible telephony denial-of-service attacks targeting PSAPs' administrative (non-911) telephone lines.

- The FBI's Internet Crime Complaint Center has also provided alerts to PSAPs. For example, in April 2013, the FBI's Internet Crime Complaint Center warned PSAPs about telephony denial-of-service attacks targeting them and advised victims to report incidents to law enforcement. The advisory noted that dozens of such attacks had targeted the administrative PSAP lines and that the attacks were part of an extortion scheme demanding payment for an outstanding debt to be paid to an individual or organization. The perpetrator launched an attack that inundated the PSAP with a continuous stream of calls for a lengthy period of time.

Identified Agencies Have Coordinated Cybersecurity Technical Assistance with State and Local Governments, but Efforts Are Not Generally Targeted to Public Safety Entities

DHS, Transportation, Commerce, and the FCC had coordinated with state and local governments to provide technical assistance including cybersecurity awareness training on cybersecurity threats and available resources, guidance to strengthen their cybersecurity posture, and cyber exercises and cybersecurity assessments to help them identify cyber vulnerabilities. The technical assistance was provided to public safety entities in a few instances, but was generally not targeted to them.

DHS's state and local government-focused activities included:

- Performing outreach to state governors, chief information officers, and chief information security officers to build awareness of cybersecurity threats and DHS technical resources available to them.
- Since 2010, conducting 114 cyber resilience reviews, including at least 1 that was focused on a local government's 911 and emergency management cyber operations, in order to enhance the cybersecurity posture of state and local government partners. These reviews were free, voluntary, and covered the entities' cybersecurity practices

²⁴Fusion centers are established through a collaboration of two or more federal and state agencies to receive, gather, analyze, and disseminate information intended to detect, prevent, investigate, and respond to criminal or terrorist activity. DHS's Office of Intelligence and Analysis, through its State and Local Program Office, is responsible for coordinating federal support to fusion centers.

regarding the management of assets, controls, incidents, service continuity, and risk.

- Leading 33 cyber-related exercises since 2006 with state, local, and territorial government partners to test and evaluate plans and policies to handle cyber incidents.
- Providing financial support to the Multi-State Information Sharing and Analysis Center (e.g., \$6.7 million in 2012), whose members represent the 50 states, 4 U.S. territories, 4 tribal nations, and hundreds of municipalities. Its security operations center provides intrusion prevention support services for state and local government systems by actively monitoring their networks. Currently the monitoring covers 22 states, 7 local governments, and 1 territory.
- Developing and administering, in coordination with the Multi-State Information Sharing and Analysis Center and the National Association of State Chief Information Officers, a national cybersecurity questionnaire. It was distributed to state and local governments to identify weaknesses and strengths in state and local governments' cybersecurity processes. In March 2012, DHS and the Multi-State Information Sharing and Analysis Center jointly issued the survey report that identified key challenges faced by state and local governments, including a low overall awareness of risks to their systems, a lack of information security and disaster recovery plans, and a less mature cybersecurity capability among local governments.²⁵ According to DHS officials, DHS has partnered with the Multi-State Information Sharing and Analysis Center to complete a second iteration of the survey and plans to report the results in March 2014.
- Performing outreach activities, including presentations at professional conferences on cybersecurity and related available federal resources, with organizations such as the National Emergency Management Association and the International Association of Chiefs of Police that represent public safety professionals.
- Providing, through FEMA, technical assistance to 12 state-level emergency operations centers in 2010 through 2012 that was not cybersecurity specific but could benefit public safety entities' IT infrastructure. For example, FEMA assisted states with their information sharing and coordination capability and with emergency operations center design and management functions.

²⁵DHS, *2011 Nationwide Cyber Security Review* (Washington, D.C.: March 2012).

FCC, Transportation, and Commerce have also provided technical assistance to state and local governments that was not targeted to the cybersecurity of public safety entities, but could benefit their operations.

- FCC provided technical assistance via its website to state and local governments by issuing guidelines for planning for the continuity of their PSAP operations and managing the security and operability of the PSAP communications systems and networks during emergencies. PSAPs may choose to implement the FCC guidelines, which are voluntary, to further develop, enhance, and expand their current emergency and disaster preparedness, response and recovery plans, and strategic approach to their overall emergency communications plans. According to FCC officials responsible for making the guidance available, FCC does not track the use of the guidance by PSAPs. In addition, according to local county public safety officials from one county, FCC provided technical assistance to resolve communications problems that arose due to issues with radio frequencies and signals.
- FCC worked with state and local governments to incorporate federal access control standards into FirstNet development efforts.
- Transportation and Commerce also provided technical assistance activities that, while not cybersecurity related, were intended to help enhance the technology infrastructure for PSAPs and to improve coordination and communications among federal, state, and local emergency communications systems, and others involved in the implementation of enhancements to 911 services. Specifically, the National Highway Traffic Safety Administration and NTIA jointly offer educational services and technical and operational information to state and local governments on implementing new technology such as IP-enabled 911 services.

FCC's Regulatory Oversight of Telecommunications Providers Could Benefit Public Safety Entities

FCC's regulatory oversight of the reliability and availability of telecommunications services does not directly impact state and local public safety entities. Public safety entities may benefit from FCC actions because the telecommunication providers' services are essential to the public safety entities' ability to receive emergency calls and dispatch first responders to the correct location. For example, the FCC requires reporting on telecommunications service outages, and its outage reporting guidelines include requirements to report extended service interruptions (exceeding 30 minutes) potentially affecting 911 call centers.

In addition, in June 2013, FCC established an e-mail address for PSAPs to voluntarily report communications provider outages they experience directly to the FCC.²⁶ Further, in December 2013, FCC released an order adopting new rules requiring providers to take reasonable measures to provide reliable 911 service with respect to circuit diversity, central office backup power, and diverse network monitoring.²⁷

Conclusions

Identified federal agencies coordinate to varying degrees with state and local governments about the cybersecurity of IT relied on to receive and respond to 911 communications by PSAPs, first responder agencies, and emergency operations centers. Federal cybersecurity efforts may indirectly benefit public safety entities, but their efforts are generally not targeted to them. While DHS collaborated with state and local governments for critical infrastructure planning for the emergency services sector, the current plan does not incorporate cybersecurity protections for NG 911 and the FirstNet network. Until DHS, in collaboration with stakeholders, develops the next iteration of the sector-specific plan, it is unclear if the cybersecurity implications of implementing NG 911 and the FirstNet network will be considered. As these new technologies are adopted to enhance the capabilities of public safety entities, cyber risks will increase. Thus, effective federal cybersecurity coordination including critical infrastructure protection planning with state and local governments concerning their public safety entities could better position the sector to identify and mitigate these risks.

Recommendation

We recommend that the Secretary of Homeland Security, in collaboration with emergency service sector stakeholders, address the cybersecurity implications of implementing NG 911 and the FirstNet network in the next iteration of sector plans.

²⁶On June 11, 2013, the FCC issued a public notice entitled, "FCC's Public Safety & Homeland Security Bureau Announces that Public Safety Answering Points Wishing to Report Communications Outages Directly to the Commission Can Now Do So By Email: psapreport@fcc.gov," which encourages PSAPs to voluntarily report telecommunications service outages.

²⁷*In the Matter of Improving 911 Reliability*, FCC 13-158, December 12, 2013.

Agency Comments and Our Evaluation

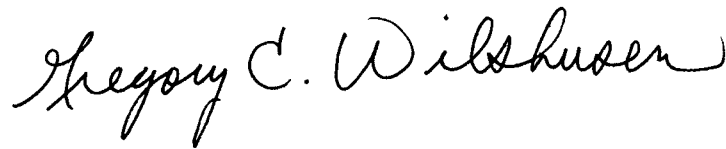
We provided a draft of this report to the Departments of Homeland Security, Commerce, Justice, and Transportation, and the Federal Communications Commission for their review and comment. DHS provided written comments on our report (see app. II), signed by DHS's Director of Departmental GAO-OIG Liaison Office. In its comments, DHS concurred with our recommendation. In addition, DHS stated that the revised NIPP was released in December 2013, and it will work with sector partners to develop an updated Emergency Services Sector-Specific Plan that will include consideration of both NG 911 and the FirstNet network. DHS estimated completing the updated sector plan by December 31, 2014.

FCC also provided written comments on a draft of our report (see app. III), signed by the Chief, Public Safety and Homeland Security Bureau. FCC stated that without coordination on public safety cybersecurity matters among federal, state, and local governments, the problems outlined in this report will not be properly addressed. Further, FCC agreed that the current Emergency Service Sector Specific Plan does not provide the detail necessary to address the threat.

Audit liaisons from DHS, FCC, and Justice also provided technical comments via e-mail. We incorporated these comments where appropriate.

We are sending copies of this report to interested congressional committees; the Secretaries of the Departments of Commerce, Homeland Security, and Transportation; the Attorney General of the United States; the Chairman of the Federal Communications Commission; the Director of the Office of Management and Budget; and other interested parties. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent 'G' and 'W'.

Gregory C. Wilshusen
Director
Information Security Issues

List of requesters

The Honorable Fred Upton
Chairman
The Honorable Henry Waxman
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Greg Walden
Chairman
The Honorable Anna Eshoo
Ranking Member
Subcommittee on Communications and Technology
Committee on Energy and Commerce
House of Representatives

The Honorable Diana DeGette
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

Appendix I: Objective, Scope, and Methodology

Our objective was to determine the extent to which federal agencies coordinated with state and local governments regarding cybersecurity efforts at emergency operations centers, public safety answering points, and first responder agencies involved in handling emergency calls.

The scope of our audit focused on identified federal agencies that have a role and responsibilities for coordinating cybersecurity efforts with state and local governments. We also included state and local governments and related public safety entities and key industry associations that are involved in handling emergency calls or work closely with or represent those in the emergency communications industry.

To identify the roles of federal agencies and select the organizations responsible for coordinating cybersecurity efforts with state and local government for public safety entities, we reviewed relevant federal law, policy, regulation, and critical infrastructure protection-related strategies, including the following:

- Homeland Security Act of 2002;
- Middle Class Tax Relief and Job Creation Act of 2012;
- Implementing Recommendations of the 9/11 Commission Act of 2007;
- 2009 National Infrastructure Protection Plan;
- 2010 Emergency Services Sector-Specific Plan;
- 2012 Emergency Services Sector Cyber Risk Assessment;
- 2003 National Strategy to Secure Cyberspace;
- Department of Homeland Security's Information Sharing Strategy, January 2013;
- Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, February 12, 2013;
- Executive Order 13618—Assignment of National Security and Emergency Preparedness Communications Functions, July 6, 2012;
- Executive Order 13636—Improving Critical Infrastructure Cybersecurity, February 19, 2013; and
- Title 47, Code of Federal Regulations sections 4.5, 4.9, 12.3, and Part 400.

We analyzed these documents to identify federal agencies responsible for coordinating with state and local governments regarding cybersecurity-related activities, including partnering with state and local government emergency services organizations to fulfill planning and assessment efforts, providing technical assistance, and sharing relevant information about threat, vulnerabilities, and mitigation techniques. In addition, we analyzed these documents to determine other methods that could support the cybersecurity of emergency services to include administering grants

related to improving 911 services or regulating essential functions such as communications. Based on our analysis, we determined that the Departments of Homeland Security, Commerce, Justice, and Transportation and the Federal Communications Commission were key federal entities relevant to our objective and identified five key activities related to cybersecurity coordination, to evaluate the federal entities against: (1) supporting critical infrastructure protection-related planning, (2) issuing grants, (3) sharing information, (4) providing technical assistance, and (5) regulating and overseeing essential functions.

To determine the identified federal entities' cybersecurity coordination activities related to these activities, we collected and analyzed relevant plans and reports dated from 2009 to 2013. For example, we analyzed DHS's State, Local, Tribal and Territorial Cybersecurity Engagement Program efforts to build partnerships with their non-federal partners to advance DHS's mission in protecting critical network systems. To get a better understanding of grants and how they are issued, we analyzed the Federal Emergency Management Agency's guidance on public safety grant funds, Transportation's administration of the E911 grant program, and the Justice's reports on Office of Justice Program grantees. To determine the responsibilities of various agencies in regulating and overseeing functions, we analyzed various laws to determine DHS responsibilities to state and local entities and Federal Communications Commission's outage reporting requirements. In addition, we interviewed officials from Department of Homeland Security's Office of Cybersecurity and Communications, Office of Infrastructure Protection, and the Federal Emergency Management Agency; Commerce's National Telecommunications and Information Administration, and First Responder Network Authority; Justice's Federal Bureau of Investigation, Justice Management Division, and Community Oriented Policing Services; Transportation's National Highway Traffic Safety Administration; and the Federal Communications Commission's Public Safety and Homeland Security Bureau.

To confirm federal efforts and gain an understanding regarding how public safety entities operate, we analyzed relevant policies, plans, and reports such as the National Emergency Number Association's Primer on the 911 Call Process, Recommended Best Practices Checklist Against TDoS Attacks, and Emergency Number Professional's Reference Manual; the California 911 Emergency Communications Office's explanation of E911 Call Flow; the Metropolitan Washington Councils of Governments Final Report on 911 Service Gaps During and Following the Derecho Storm on June 29, 2012; the Federal Communications

Commission's report on Impact of the June 2012 Derecho on Communications Networks and Services, and How 911 Works by Julia Layton. In addition, we interviewed officials familiar with emergency operations and/or cybersecurity aspects of state and local governments from the National Association of State Chief Information Officers; National Emergency Number Association; National Emergency Managers Association; National Association of State 911 Administrators; Multi-State Information Sharing and Analysis Center; International Association of Fire Chiefs; and the National Governors Association.

We also interviewed state and local government officials familiar with emergency communication operations based on proximity of location, leadership in national associations, and/or involvement in ongoing technology enhancements. For example, we interviewed public safety officials from the Alabama 911 Board; Arlington County, Virginia; California Public Safety Communications Office; Fairfax County, Virginia; Orange County, California; Overland Park, Kansas; and Wake County, North Carolina. In addition, to get a better understanding of cybersecurity and the activities performed at public safety answering points and emergency operations centers and their interaction with first responders, we reviewed and analyzed the operations and responsibilities of the California Technology Agency Public Safety Communications Office, and observed the operations of the McConnell Public Safety and Transportation Operations Center in Fairfax County, Virginia, and the Arlington County Emergency Communications Center in Arlington, Virginia.

We determined that information provided by the federal, state, and local agencies, such as plans, guideline, and manuals, was sufficiently reliable for the purposes of our review. To arrive at this assessment, we corroborated the information by comparing it with statements from relevant agency officials.

We conducted this performance audit from November 2012 to January 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

January 16, 2014

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO 14-125, "CRITICAL INFRASTRUCTURE PROTECTION: More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO recognized DHS coordination with state and local governments, through the Emergency Services Sector Coordinating Council, in the development of a plan for protection of emergency services critical infrastructure and key resources. DHS is committed to infrastructure security and resilience through stakeholder engagement.

The report also noted that current federal cybersecurity efforts benefit public safety entities and DHS spearheaded coordination with the sector; however, current sector plans do not address protective measures for two specific tools: next generation of 9-1-1 services (NG 911) and public safety broadband. In addition, neither the Nationwide Public Safety Broadband Network (NPSBN), currently being deployed by the First Responder Network Authority (FirstNet), nor NG 911 had been established when the Emergency Services Sector-Specific Plan was released in 2010. It is important to also note, however, that in December 2013, DHS published the latest iteration of the National Infrastructure Protection Plan (NIPP): *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. The NIPP integrates core cyber considerations to reflect the increasing interdependency of security and resilience, both physical and cyber.

With the release of the updated NIPP, DHS will begin working with partners across all sectors, including the Emergency Services Sector, to update the sector-specific plans. The updated plan for the Emergency Services Sector will include consideration of both NG 911 and the NPSBN.

While the Emergency Services Sector-Specific Plan does not currently address NG 911 and public safety broadband, the Department has worked with public safety on several initiatives to assist stakeholders in ensuring new technology is appropriately secure and resilient. DHS collaborated with public and private entities to develop an Emergency Services Sector Cyber

Risk Assessment in 2012. The Assessment provides a risk profile to enhance the security and resilience of the Emergency Services Sector disciplines. It is an effort to establish a baseline of cyber risks across the sector, to ensure federal resources are applied where they offer the most benefit for mitigating risk, and to encourage a similar risk-based allocation of resources within state and local entities and the private sector. Emergency managers from local, state, and Federal Government actively participated in the development process to ensure the assessment provided practical guidance for the public safety community.

As a member of the FirstNet Board, DHS has also been active in the development and deployment of the NPSBN. The development and deployment of an Internet protocol-based network for public safety will represent a leap forward in communications capabilities for first responders, law enforcement, and other users of the NPSBN. However, the move to such a network presents a challenge for the emergency management community in identifying threats to and vulnerabilities of cyber infrastructure in the network that could affect the network's reliability and security. DHS is working with FirstNet and the public safety community to identify cyber risks and develop potential responses to those risks. In 2013, DHS, through the National Protection and Programs Directorate's (NPPD's) Office of Emergency Communications, developed the NPSBN Cyber Infrastructure Risk Assessment to provide FirstNet with a how-to guide addressing the top cyber risks that the network may face. DHS is now working with FirstNet to ensure a more resilient network design that will integrate security and resilience into the overall physical and cyber aspects of the NPSBN.

In addition, DHS has been providing operational support to 9-1-1 centers and public safety entities related to Telephonic Denial of Service (TDOS) attacks. Some 9-1-1 centers have been targeted by TDOS attacks that overwhelm Public Safety Answering Points' administrative lines. These attacks inundate a 9-1-1 call center with a high volume of calls, overwhelming the system's ability to process calls and impeding the system from receiving legitimate calls. DHS, through NPPD's Office of Cybersecurity and Communications (CS&C) National Cybersecurity & Communications Integration Center (NCCIC), has worked on the development and dissemination of techniques for mitigating and managing these TDOS attacks, which will allow emergency management agencies to continue to provide these critical services to the public.

DHS is committed to working with both the public safety community as well as our partners in the Federal Government to ensure new and emerging technology is secure and resilient.

The draft report contained one recommendation with which the Department concurs. Specifically, GAO recommended the Secretary of Homeland Security, in collaboration with emergency services sector stakeholders:

Recommendation: Address the cybersecurity implications of implementing NG 911 and the FirstNet network in the next iteration of sector plans.

Response: Concur. As the sector-specific agency for the emergency services sector, DHS is responsible for supporting sector identification of vulnerabilities. The updated Emergency Services Sector-Specific Plan is estimated to be completed by the end of 2014. Building on

existing initiatives, NPPD will work with public safety entities to develop the updated plan, including addressing vulnerabilities to new and emerging technologies, such as NG 911 and public safety broadband. Estimated Completion Date: December 31, 2014.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumacker
Director
Departmental GAO-OIG Liaison Office

Appendix III: Comments from the Federal Communications Commission



Federal Communications Commission
Washington, D.C. 20554

January 16, 2014

Mr. Michael W. Gilmore
Assistant Director
Information Technology Team
Government Accountability Office
441 G Street NW
Washington, DC 20548

**Re: CRITICAL INFRASTRUCTURE PROTECTION: More
Comprehensive Planning Would Enhance the Cybersecurity of Public Safety
Entities' Emerging Technology (GAO-14-125)**

Dear Mr. Gilmore:

Thank you for the opportunity to review the United States Government Accountability Office's (GAO's) draft Report to Congressional Requesters entitled "More Comprehensive Planning Would Enhance the Cybersecurity of Public Safety Entities' Emerging Technology."

The Federal Communications Commission (FCC) takes the security of our Nation's communications networks seriously. The FCC advisory committee that covers cybersecurity is the Communications Security, Reliability, and Interoperability Council (CSRIC). CSRIC recommends and promotes the implementation of cybersecurity best practices to secure the underlying Internet infrastructure. The best practices have resulted in improved security for communications technologies, including mobile; however, they have not yet comprehensively closed the cyber readiness shortfall central to your review.

The FCC coordinates on public safety cybersecurity matters with the Department of Homeland Security, State and Local Governments that operate Public Safety Answering Points (PSAPs), and industry which together make up the public safety communications ecosystem. Without coordination of these entities, the problems outlined in this report will not be properly addressed.

**Appendix III: Comments from the Federal
Communications Commission**

We agree that the current Department of Homeland Security *Emergency Service Sector Specific Plan* does not provide the detail necessary to address the threat. Future Plans need to include the FCC and other regulatory agencies from the beginning to ensure that the regulatory structure provides the proper incentives to “bake” security into architectures in an effective and accountable manner.

Again, thank you for the opportunity to review the draft report.

Sincerely,

A handwritten signature in black ink, appearing to read "D. G. Simpson", written over a horizontal line.

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

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

GAO staff who made significant contributions to this report include Michael W. Gilmore, Assistant Director; Nancy Glover; Barbarol James; Kenneth A. Johnson; David Plocher; and Adam Vodraska.

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](#).
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

