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

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.