GAO
Highlights

Highlights of GAO-15-749, a report to congressional committees

July 2015

DEFENSE INFRASTRUCTURE

Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning

Why GAO Did This Study

Continuity of operations at DOD installations is vital to supporting the department's missions, and the disruption of utility services—such as electricity and potable water, among others—can threaten this support. House Report 113-446 included a provision that GAO review DOD's and the military services' actions to ensure mission capability in the event of disruptions to utility services. This report addresses (1) whether threats and hazards have caused utility disruptions on DOD installations and, if so, what impacts they have had; (2) the extent to which DOD's collection and reporting on utility disruptions is comprehensive and accurate; and (3) the extent to which DOD has taken actions and developed and implemented guidance to mitigate risks to operations at its installations in the event of utility disruption. For this review, GAO evaluated DOD guidance and policies, interviewed appropriate officials, and visited or contacted 20 installations within and outside the continental United States, selected based on criteria to include those experiencing multiple disruptions, disruptions of more than one type of utility, and each military service.

What GAO Recommends

GAO recommends that DOD work with the services to clarify utility disruption reporting guidance, improve data validation steps, and address challenges to addressing cybersecurity ICS guidance. DOD concurred or partially concurred with all but one recommendation and disagreed with some of GAO's analysis. GAO believes the recommendations and analysis are valid as discussed in the report.

View GAO-15-749. For more information, contact Brian J. Lepore at (202) 512-4523 or leporeb@gao.gov.

What GAO Found

Department of Defense (DOD) installations have experienced utility disruptions resulting in operational and fiscal impacts due to hazards such as mechanical failure and extreme weather. Threats, such as cyber attacks, also have the potential to cause disruptions. In its June 2014 Annual Energy Management Report (Energy Report) to Congress, DOD reported 180 utility disruptions lasting 8 hours or longer, with an average financial impact of about $220,000 per day, for fiscal year 2013. Installation officials provided specific examples to GAO, such as at Naval Weapons Station Earle, New Jersey, where in 2012, Hurricane Sandy's storm surge destroyed utility infrastructure, disrupting potable and wastewater service and resulting in almost $26 million in estimated repair costs. DOD officials also cited examples of physical and cyber threats, such as the "Stuxnet" computer virus that attacked the Iranian nuclear program in 2010 by destroying centrifuges, noting that similar threats could affect DOD installations.

DOD's collection and reporting of utility disruption data is not comprehensive and contains inaccuracies, because not all types and instances of utility disruptions have been reported and there are inaccuracies in reporting of disruptions' duration and cost. Specifically, in the data call for the Energy Reports, officials stated that DOD installations are not reporting all disruptions that meet the DOD criteria of commercial utility service disruptions lasting 8 hours or longer. This is likely due, in part, to military service guidance that differs from instructions for DOD's data collection template. In its Energy Reports, DOD is also not including information on disruptions to DOD-owned utility infrastructure. There also were inaccuracies in the reported data. For instance, $4.63 million of the $7 million in costs reported by DOD in its June 2013 Energy Report were indirect costs, such as lost productivity, although DOD has directed that such costs not be reported. Officials responsible for compiling the Energy Report noted that utility disruption data constitutes a small part of the report and they have limited time to validate data. However, without collecting and reporting complete and accurate data, decision makers in DOD may be hindered in their ability to plan effectively for mitigating against utility disruptions and enhance utility resilience, and Congress may have limited oversight of the challenges these disruptions pose.

Military services have taken actions to mitigate risks posed by utility disruptions and are generally taking steps in response to DOD guidance related to utility resilience. For example, installations have backup generators and have conducted vulnerability assessments of their utility systems. Also, DOD is in the planning stages of implementing new cybersecurity guidance, by March 2018, to protect its industrial control systems (ICS), which are computer-controlled systems that monitor or operate physical utility infrastructure. Each of the military services has working groups in place to plan for implementing this guidance. However, the services face three implementation challenges: inventorying their installations' ICS, ensuring personnel with expertise in both ICS and cybersecurity are trained and in place, and programming and identifying funding for implementation. For example, as of February 2015, none of the services had a complete inventory of ICS on their installations. Without overcoming these challenges, DOD's ICS may be vulnerable to cyber incidents that could degrade operations and negatively impact missions.