



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.

DEFENSE INFRASTRUCTURE

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

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.

Contents

Letter		1
	Background	7
	Hazards Caused Utility Disruptions Resulting in Operational and Fiscal Impacts; Physical and Cyber Threats Pose Similar Impacts	11
	DOD Collects and Reports Utility Disruption Data, but Its Data Are Not Comprehensive and Some Are Not Accurate	20
	The Military Services Have Taken Actions and Implemented DOD Guidance to Mitigate Risks of Utility Disruptions but Face Challenges in Implementing Cybersecurity Guidance for Industrial Control Systems	31
	Conclusions	45
	Recommendations for Executive Action	46
	Agency Comments and Our Evaluation	47
Appendix I	Scope and Methodology	52
Appendix II	Previous GAO Work on the Vulnerabilities of Utility Infrastructure	58
Appendix III	Comments from the Department of Defense	61
Appendix IV	GAO Contact and Staff Acknowledgments	64
Related GAO Products		65
Tables		
	Table 1: Selected DOD Guidance Related to Mitigating Risk to Operations at Installations in the Event of Utility Disruptions and Summary of Our Analysis of Implementation Efforts by Installations in Our Sample	34
	Table 2: Installations Visited or Contacted	53

Figures

Figure 1: Industrial Control System (ICS) Cyber Incidents in the Energy and Water and Wastewater Sectors Reported to the Department of Homeland Security Industrial Control System Cyber Emergency Response Team from 2009 to 2014	10
Figure 2: Number of Utility Disruptions Reported by DOD Components to the Office of the Secretary of Defense (OSD), Fiscal Years 2012 through 2014	13
Figure 3: Information on Disruptions Lasting 8 Hours or Longer, Fiscal Years 2012 through 2104, Reported to GAO by 18 DOD Installations inside and outside the Continental United States	14
Figure 4: Information on the Number of Disruptions Experienced by 18 DOD Installations inside and outside the Continental United States That Reported to GAO on Disruptions Lasting 8 Hours or Longer, from Fiscal Year 2012 through Fiscal Year 2014	15
Figure 5: Utility Pole Damaged by a Wildfire on Vandenberg Air Force Base	16
Figure 6: Repairs to a Potable-Water Pipe on Vandenberg Air Force Base	17
Figure 7: Example of a Potential Cyber Attack Using False Data in an Industrial Control System	20
Figure 8: DOD's Typical Process for Collecting the Data on Utility Disruptions Reported in Its Annual Energy Management Report	22
Figure 9: Potable and Wastewater Infrastructure at Naval Weapons Station Earle Destroyed by Hurricane Sandy, and New, Strengthened Water Lines Being Installed	33
Figure 10: Video Still Photo Showing Physical Damage to Generator during Cyber Attack Test by Idaho National Laboratory	37

Abbreviations

DOD	Department of Defense
ICS	Industrial Control System
OSD	Office of the Secretary of Defense

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.



July 23, 2015

Congressional Committees

Department of Defense (DOD) installations serve as platforms from which the department employs forces across the full spectrum of military operations. To accomplish their missions, DOD installations inside and outside the continental United States must have assurance that they can continue to operate in the face of man-made and weather-induced utility interruptions that affect electric, potable water, wastewater, and natural gas services.¹ According to DOD, threats such as cyber attacks on industrial control systems (ICS)² and hazards such as severe weather events³ are a risk to ensuring the reliable provision of utility services to its installations. For example, in a March 2014 memorandum, DOD noted that cyber infiltration through ICS used to control and monitor utilities could result in a serious mission-disabling event.⁴ Specifically, ICS could be used as a gateway into the installation’s information technology system or possibly DOD’s broader information networks. In addition, DOD’s April 2015 Cyber Strategy states that adversaries can target utilities’ ICS and cyber attacks could present a significant risk to national

¹For the purposes of this report, *potable water* refers to drinking water, while *wastewater* refers to sewage and—in some cases—storm water. The storm sewer and wastewater infrastructure are considered to be separate systems on some DOD installations, and single systems on other installations.

²ICS are computer-controlled systems that monitor or operate physical utility infrastructure, among other things. ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as skid-mounted Programmable Logic Controllers often found in the industrial sectors and critical infrastructures, including utility systems.

³For the purposes of this report, we define “threats” and “hazards” using definitions in DOD Directive 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure* (Sept. 21, 2012). Specifically, a threat is an adversary that has the intent, capability, and opportunity to cause loss or damage. Hazards are nonhostile incidents such as accidents, natural forces, and technological failure that cause loss or damage to infrastructure assets.

⁴Memorandum from the Acting Deputy Under Secretary of Defense for Installations and Environment, Subject: *Real Property-related Industrial Control System Cybersecurity* (Mar. 19, 2014).

security.⁵ Also, according to March 2014 congressional testimony given by DOD, extreme weather events—such as hurricanes—have caused utility disruptions that can affect mission continuity.⁶ Further, climate change increases the likelihood of such events and DOD must be prepared for—and have the ability to recover from—utility disruptions that impact mission continuity on DOD installations.⁷

In recent years, a number of DOD efforts have highlighted the importance of utility resilience—the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions caused by deliberate attacks, accidents, or naturally occurring events. In addition to the memorandum discussed above, two recent memorandums direct DOD components to define future power resilience requirements⁸ and to take steps to ensure that adequate measures have been taken to plan, prepare, and provide for an adequate water supply, which installations depend on to fulfill their missions.⁹ In addition, DOD has issued two Climate Change Adaptation Road Maps, which outline the potential impacts of climate change on utility infrastructure and service, and contain possible courses of action to address these impacts.

⁵Department of Defense, *The Department of Defense Cyber Strategy* (Washington, D.C.: April 2015).

⁶John Conger, Acting Deputy Under Secretary of Defense for Installations and Environment, testimony before the Subcommittee on Military Construction, Veteran Affairs, and Related Agencies, Committee on Appropriations, House of Representatives, 113th Cong., 2nd sess., March 12, 2014.

⁷According to DOD, climate change is any given change in climate over time, whether due to natural variability or as a result of human activity. In May 2014, we found that while it is not possible to link any individual weather event to climate change, these events provide insight into the potential climate-related vulnerabilities the United States faces. We also reported that, according to DOD installation-level officials, the department's facilities and infrastructure are vulnerable to climate change phenomena. Further, these officials recognized that climate change may make these types of phenomena more frequent or severe. See GAO, *Climate Change Adaptation: DOD Can Improve Infrastructure Planning and Processes to Better Account for Potential Impacts*, [GAO-14-446](#) (Washington, D.C.: May 30, 2014).

⁸Memorandum from the Acting Deputy Under Secretary of Defense for Installations and Environment, *Department of Defense Electric Power Resilience* (Dec. 16, 2013).

⁹Memorandum from the Acting Deputy Under Secretary of Defense for Installations and Environment, *Water Rights and Water Resources Management on Department of Defense Installations and Ranges in the United States and Territories* (May 23, 2014).

In addition, we have identified two key utility resilience issue areas as high-risk areas for the federal government.¹⁰ Since 1997, the security of federal cyber assets has been on our list of high-risk areas and we have found that the federal government continues to face challenges in effectively implementing cybersecurity policies. GAO and agency inspector general reports have identified challenges in a number of key areas of the government's approach to cybersecurity including those related to protecting government information and systems and the nation's critical cyber infrastructure. Also, in 2013, we added climate change to our list of high-risk areas, focusing on limiting the federal government's fiscal exposure by better managing climate change risks. In doing so, we found that climate change is considered by many to be a complex, crosscutting issue that poses risk to many environmental and economic systems and presents a significant financial risk to the federal government. In May 2014, we found that DOD's implementation of guidance directing the consideration of climate change in installation planning is likely to vary across the department and that DOD processes for approving and funding infrastructure projects did not explicitly account for climate change.¹¹ We made recommendations that DOD develop a plan and milestones for completing climate change vulnerability assessments of installations; provide further information to installation planners, clarifying actions that should be taken to account for climate change in planning documents; and clarify the processes used to compare military construction projects for funding, to include consideration of potential climate change impacts. DOD concurred with our recommendations.¹²

House Report 113-446, accompanying H.R. 4435, a bill for the National Defense Authorization Act for Fiscal Year 2015, 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. Our study examines electric, potable water, wastewater, and natural gas services at

¹⁰GAO, *High Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

¹¹[GAO-14-446](#).

¹²According to an Office of the Secretary of Defense (OSD) official, DOD is taking actions toward implementing the recommendations. For example, DOD is planning on incorporating climate change considerations into its process for conducting environmental assessments. Further, DOD is drafting a DOD Directive that addresses the responsibility for integrating climate change considerations into a variety of existing DOD guidance.

domestic and overseas military installations. 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 of information 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. This is a publicly releasable version of a report, marked for official use only, which we issued in July 2015. This report does not identify specific vulnerabilities in defense, or defense-related, structures or systems—information that DOD deemed to be sensitive. Although the information provided in this report is less detailed, it addresses the same objectives as our report marked for official use only. Also, the methodology used for both reports is the same.

To determine whether threats and hazards have caused utility disruptions on DOD installations—and if so—what impacts they have had, we reviewed various documents on utility disruptions, resulting impacts on installation operations, and interviewed officials from a nongeneralizable sample of 20 DOD installations from inside and outside the continental United States. To identify instances of utility disruptions on DOD installations, we reviewed the military services' data submissions for DOD's Annual Energy Management Reports (Energy Reports) for fiscal years 2012, 2013, and 2014.¹³ Because DOD's data in its Energy Reports do not provide specific examples of disruptions and their impacts, we conducted independent research using publicly available information, such as news articles, the details of which we then asked officials from the military services to verify. We chose to collect data from 2005 to 2014 for the purposes of collecting a large number of examples of utility disruptions and their impacts. Further, we used our data and DOD's data to choose the 20 installations to include in a nongeneralizable sample. Our selection was based on whether an installation had more than one instance of utility disruption, or had a disruption of multiple types of utility service; and we chose installations from each military service. To each

¹³According to GAO analysis of information provided by an OSD official, the military services account for about 87 percent of the utility disruptions reported to OSD for fiscal years 2012 to 2014. Because their installations account for a large majority of reported disruptions, we focus on the military services' utility disruptions in this report. At the time of our review, OSD had collected and reviewed the fiscal year 2014 data, but had not yet published the report. DOD published the fiscal year 2014 report in May 2015..

installation, we sent questions regarding the instances of utility disruptions identified in our research and the impacts of those disruptions. From the 20 installations, we gathered information on utility disruptions and their impacts; actions they had taken to mitigate such impacts; and implementation of selected pieces of DOD utility resilience guidance, discussed in more detail below. The installations in our sample provided information on utility disruptions from 2005 to 2014, lasting 8 hours or longer. In our sample of 20 installations, 18 installations reported disruptions lasting 8 hours or longer that occurred in fiscal years 2012, 2013, or 2014; and 2 installations reported disruptions lasting 8 hours or longer that occurred prior to fiscal year 2012. Although the information we collected was not representative of all installations, we determined that these data were sufficiently reliable for the purposes of presenting the number and certain characteristics of utility disruptions, as reported by the installations' officials. Table 2 in appendix I lists the installations we visited or contacted and their locations.

To determine the extent to which DOD's collection and reporting of information on utility disruptions is comprehensive and accurate, we reviewed the statutory reporting requirement, compared the military services' data submissions in response to the requirement in fiscal years 2012 through 2014 with information we collected independently, and reviewed DOD's process for collecting and reporting on this data. For its annual Energy Reports, DOD is statutorily required to report on—among other things—the total number and location of utility outages on installations. To respond to this requirement, the military services provide information to the Office of the Secretary of Defense (OSD). We reviewed the military services' submissions of utility disruption data to OSD for fiscal years 2012 through 2014,¹⁴ as well as the June 2013 and June 2014 Energy Reports in which DOD reported these data. We reviewed these two reports because, at the time of our review, DOD had not yet issued its June 2015 report. To identify the comprehensiveness of DOD's reporting, we compared the military services' data submissions to OSD with the independent research we conducted in support of our efforts to determine whether threats and hazards have caused utility disruptions on DOD installations—and, if so, what impacts have they had. When comparing the data from our sample with the military service data submitted to DOD, we included only the disruptions that occurred on the

¹⁴This reporting requirement began in fiscal year 2012.

sample's installations from fiscal years 2012 through 2014. We also reviewed documents on, and met with military service headquarters and OSD officials about, data reporting instructions and the processes to collect, validate, and report the data. To assess the accuracy of DOD's reporting, we reviewed utilities disruption data submitted by the military services to OSD, discussed the data validation processes used by officials at both the military services' headquarters and OSD, and reviewed OSD data validation documentation. We compared DOD's processes for the collection, validation, reporting, and use of these data to several leading practices for the use and management of data and process improvement.¹⁵

To determine 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, we collected and reviewed DOD documents related to actions taken to mitigate risks, utility resilience guidance, and implementation efforts. We collected these documents from the 20 installations in our nongeneralizable sample and from the military service headquarters. We reviewed documents describing mitigation actions, such as installing and maintaining backup generators; and installations' plans, such as emergency management plans, for situations in which utility service is disrupted. We reviewed guidance related to utility resilience, which covers topics such as installation energy management, defense critical infrastructure protection, and cybersecurity and documentation describing the installations' implementation of the guidance, to include vulnerability analyses that cover all threats and hazards. Also, we met with officials from the military services' and DOD's offices of the Chief Information Officer, officials from the military services' headquarters offices, and OSD to discuss actions DOD had taken to begin implementation of the cybersecurity guidance and challenges regarding implementation. Finally, we compared DOD's implementation

¹⁵Sources for these leading practices include: (1) GAO, *Auditing and Financial Management: Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999); (2) our previous work that discusses improvement of infrastructure planning processes to better account for climate change impacts and improvement in the accuracy and completeness of data used to meet reporting requirements; see [GAO-14-446](#) and GAO, *Depot Maintenance: Accurate and Complete Data Needed to Meet DOD's Core Capability Reporting Requirements*, [GAO-14-777](#) (Washington, D.C.: Sept. 18, 2014); and (3) Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, 5th ed. (2013). PMBOK is a trademark of the Project Management Institute, Inc.

actions related to cybersecurity guidance with the implementation goals described in the guidance. More information on the scope and methodology of our research is provided in appendix I.

We conducted this performance audit from June 2014 to July 2015, 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DOD Installations Depend on Utility Services from a Variety of Sources

According to testimony from the Assistant Secretary of Defense for Energy, Installations and Environment, the use of electricity, natural gas, and other utilities is a fundamental characteristic of the nearly 300,000 buildings that DOD owns and operates. These buildings reside on over 500 major installations in the United States and overseas, which provide effective platforms for the training, deployment, redeployment, and support for the military forces that provide for the country's defense. Installation utilities expenditures are included in the operations and maintenance budget request for Base Operations, and DOD spends a substantial amount of money on utility service. For example, according to DOD, the department spent \$4.2 billion on facilities energy in fiscal year 2014.

DOD installations obtain utility services in a variety of ways, such as from commercial utility providers or on-site generation.¹⁶ For example, DOD installations typically acquire electricity and natural gas service through a

¹⁶DOD distinguishes facility energy from operational energy. Facility energy includes energy needed to power fixed installations. Operational energy is the energy required for training, moving, and sustaining military forces and weapons platforms for military operation. The scope of this report includes facility energy, but not operational energy.

public or private-sector utility provider.¹⁷ However, DOD installations may also produce some of their own electricity through on-site power generation or through the use of renewable energy projects. For water and wastewater services, DOD maintains and operates wastewater and drinking water treatment facilities on many of its installations. DOD installations may also obtain potable water by purchasing it from a water utility provider as well as from fresh water sources such as wells and streams. In addition, DOD may contract with a local wastewater treatment facility to manage wastewater.

DOD Roles and Responsibilities for Management of Utility Services on DOD Installations

Within DOD, the military departments are responsible for installation management, with oversight by the Office of the Assistant Secretary of Defense for Energy, Installations and Environment, who reports to the Under Secretary of Defense for Acquisition, Technology and Logistics.¹⁸ The former office is responsible for—among other things—issuing facility energy policy and guidance to DOD components and coordinating all congressional reports related to facility energy, including the Energy Reports. In addition, each military department is responsible for developing policies and managing programs related to energy and utility management, and has assigned a command or headquarters to execute these responsibilities.¹⁹ At the installation level, the public works, general facilities, or civil engineering departments oversee and manage the day-to-day operations of the utilities.

¹⁷We have previously found that DOD depends overwhelmingly on the U.S. commercial electrical power grid for electricity to support its operations and missions. See GAO, *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets*, [GAO-10-147](#) (Washington, D.C.: Oct. 23, 2009).

¹⁸In December 2014, the Office of the Deputy Under Secretary of Defense for Installations and Environment merged with the Office of the Assistant Secretary of Defense for Operational Energy. As a result, the offices are now called the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment, and the position of Deputy Under Secretary of Defense for Installations and Environment became the Assistant Secretary of Defense for Energy, Installations, and Environment. Because the office is currently called the Office of the Assistant Secretary of Defense for Energy, Installations and Environment, we use that title throughout this report.

¹⁹Within the Army, the responsible organization is the Installation Management Command, under the Assistant Secretary of the Army Installations and Environment; within the Navy, the Naval Facilities Engineering Command, under the Commander, Navy Installations Command; within the Marine Corps, Marine Corps Installation Command; and within the Air Force, the Air Force Civil Engineer.

DOD Collaborates with Various Federal Agencies with Responsibilities for Protecting Critical Utility Infrastructure

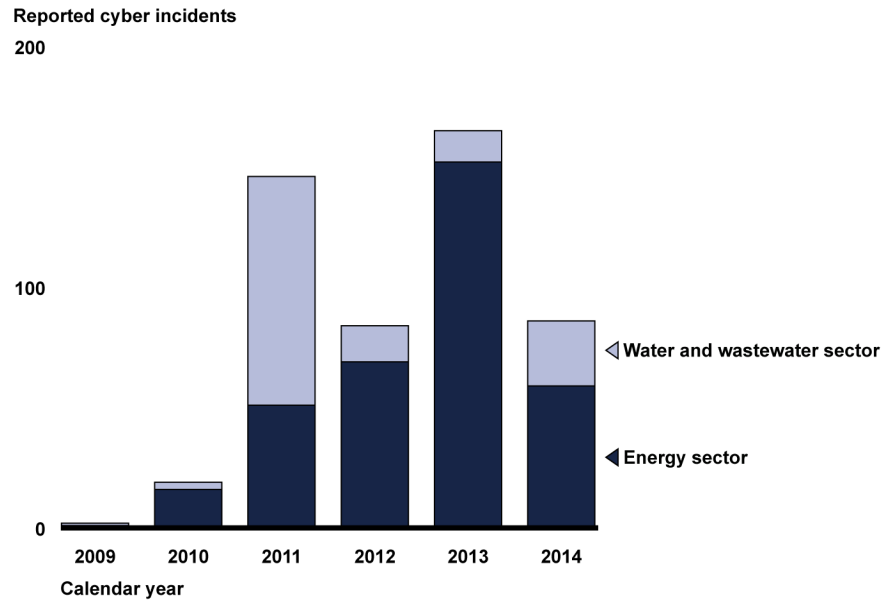
DOD collaborates with various federal agencies to manage the security of crucial utility infrastructure on which DOD relies for utility service. Managing the security of the nation's critical utility infrastructure requires collaboration among government agencies, industry groups, and private companies. Various federal departments and agencies are designated as sector-specific agencies and play a key role in critical infrastructure security and resilience activities. Specific to the utilities that are the subject of this report, the Department of Energy is the sector-specific agency responsible for the energy sector. The energy sector includes the production, refining, storage, and distribution of oil, natural gas, and electric power, except for commercial nuclear power facilities. In addition, the Environmental Protection Agency is the sector-specific agency responsible for the water and wastewater sector. The Department of Homeland Security, pursuant to Presidential Policy Directive 21, is to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure from all hazards.²⁰ For more information on GAO's previous work examining federal efforts to protect critical infrastructure and recommendations we have made to improve these efforts, see appendix II.

Cybersecurity Concerns, Industrial Control Systems, and Their Role on DOD Installations

According to DOD's April 2015 Cyber Strategy, the department will work with the Department of Homeland Security to improve cybersecurity of critical infrastructure to protect the U.S. homeland and vital interests from disruptive or destructive cyber attacks. In addition to its role in coordinating federal efforts to protect critical infrastructure, the Department of Homeland Security is responsible for leading efforts to protect the nation's cyber-reliant critical infrastructures, which includes ICS. One of its means to do this is the Industrial Control System Cyber Emergency Response Team, which has been receiving reports about cyber incidents on federal and civilian ICS since 2009. Figure 1 shows reported cyber incidents in the energy, and water and wastewater, sectors since 2009.

²⁰Executive Office of the President, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (Washington, D.C.: Feb. 12, 2013). This directive defines resilience as the ability of critical infrastructure to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, and is an area that may be included in vulnerability assessments to determine the extent to which critical infrastructure is prepared to withstand and recover from disruptions such as exposure to a given hazard or incidents arising from the deliberate exploitation of a vulnerability.

Figure 1: Industrial Control System (ICS) Cyber Incidents in the Energy and Water and Wastewater Sectors Reported to the Department of Homeland Security Industrial Control System Cyber Emergency Response Team from 2009 to 2014



Source: GAO analysis of Department of Homeland Security data. | GAO-15-749

On DOD installations, ICS are associated primarily with infrastructure, and consist of computer-controlled electromechanical systems that ensure installation infrastructure services—such as utility service—are delivered when and where required to accomplish the mission. Examples include electric infrastructure, for which ICS control actions such as opening and closing switches; for water pipes, opening and closing valves; and for buildings, operating the heating, ventilation, and air conditioning systems. Thus, many DOD missions depend on the unflinching functioning of ICS and therefore on the security of those systems. Further, DOD’s ICS have become increasingly networked and interconnected with other DOD networks and thereby potentially at risk of cyber intrusion or attack. According to DOD’s April 2015 Cyber Strategy, DOD’s own networks and systems are vulnerable to intrusions and attacks. In addition to DOD’s own networks, a cyber attack on the critical infrastructure and key resources on which DOD relies for its operations could impact the U.S. military’s ability to operate in a contingency.

Hazards Caused Utility Disruptions Resulting in Operational and Fiscal Impacts; Physical and Cyber Threats Pose Similar Impacts

DOD and selected installations reported utility disruptions for fiscal years 2012 through 2014; hazards and threats have the potential to cause utility disruptions, with operational and fiscal impacts.

DOD and Selected Installations Reported Utility Disruptions for Fiscal Years 2012 through 2014

Section 2925 of Title 10 of the United States Code requires DOD to report to Congress on a number of facility energy requirements. One of the required reporting elements is to report on utility disruptions on military installations, including—among other things—the total number and location of utility outages on installations, their financial impact, and mitigation measures. This information is reported in DOD’s annual Energy Reports. DOD components, including the four military services, provide OSD with information on utility disruptions that occurred on their installations in a given fiscal year, which OSD compiles for reporting in the Energy Reports.²¹ According to DOD, the June 2013 and June 2014 Energy Reports contain information on disruptions that occurred in fiscal years 2012 and 2013, respectively; that lasted 8 hours or longer; and were the result of interruptions in external, commercial utility service.²²

²¹We provide more information on this process later in the report.

²²As discussed in more detail later in this report, the services collect data on utility disruptions according to OSD instructions on data collection for the Energy Reports. In this report, we discuss the occurrence and impact of utility disruptions in two categories. First, disruptions to commercial utility service that is external to an installation; for example, service from a utility company. Second, disruptions to utility service provided by DOD-owned infrastructure; for example, service from potable water pipes on a DOD installation. According to OSD instructions on data collection for the Energy Reports, the services are supposed to report only utility disruptions in the first category; that is, commercial utility service that is external to an installation. We discuss these categories in more detail later in the report. Also, a proposed bill for the National Defense Authorization Act for fiscal year 2016 would, if enacted, modify the reporting requirements of section 2925 to—among other things—clarify which utility disruptions should be included in DOD’s reporting. See S. 1376, § 311 (May 19, 2015).

In its June 2013 Energy Report, DOD reported 87 disruptions and a financial impact of about \$7 million for fiscal year 2012.²³ In its June 2014 Energy Report, DOD reported 180 disruptions²⁴ and a financial impact that averaged about \$220,000 per day for fiscal year 2013.²⁵ At the time of our data collection and analysis, DOD had not issued the Energy Report with utilities disruption data from fiscal year 2014. However, OSD had collected these fiscal year 2014 data from the military services. Figure 2 summarizes the information on the number of utility disruptions reported by the military services to OSD for fiscal years 2012 through 2014.²⁶

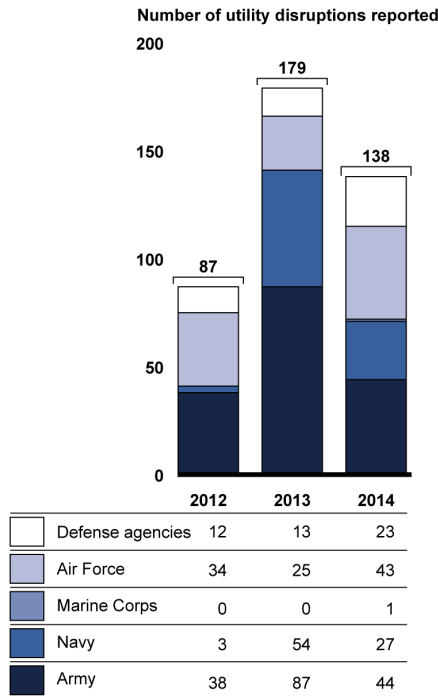
²³We discuss problems with the comprehensiveness of these data later in this report.

²⁴In June 2014, DOD reported one more utility disruption that the components reported to OSD for fiscal year 2013.

²⁵Because DOD presented fiscal years 2012 and 2013 cost information in its Energy Reports in different ways, the costs reported for these 2 fiscal years cannot be compared to each other.

²⁶According to GAO analysis of information provided by an OSD official, the military services account for almost 90 percent of the utility disruptions reported to OSD for fiscal years 2012 to 2014. Because their installations account for a large majority of reported disruptions, we focus on the military services' utility disruptions in this report, although certain defense agencies have also reported disruptions.

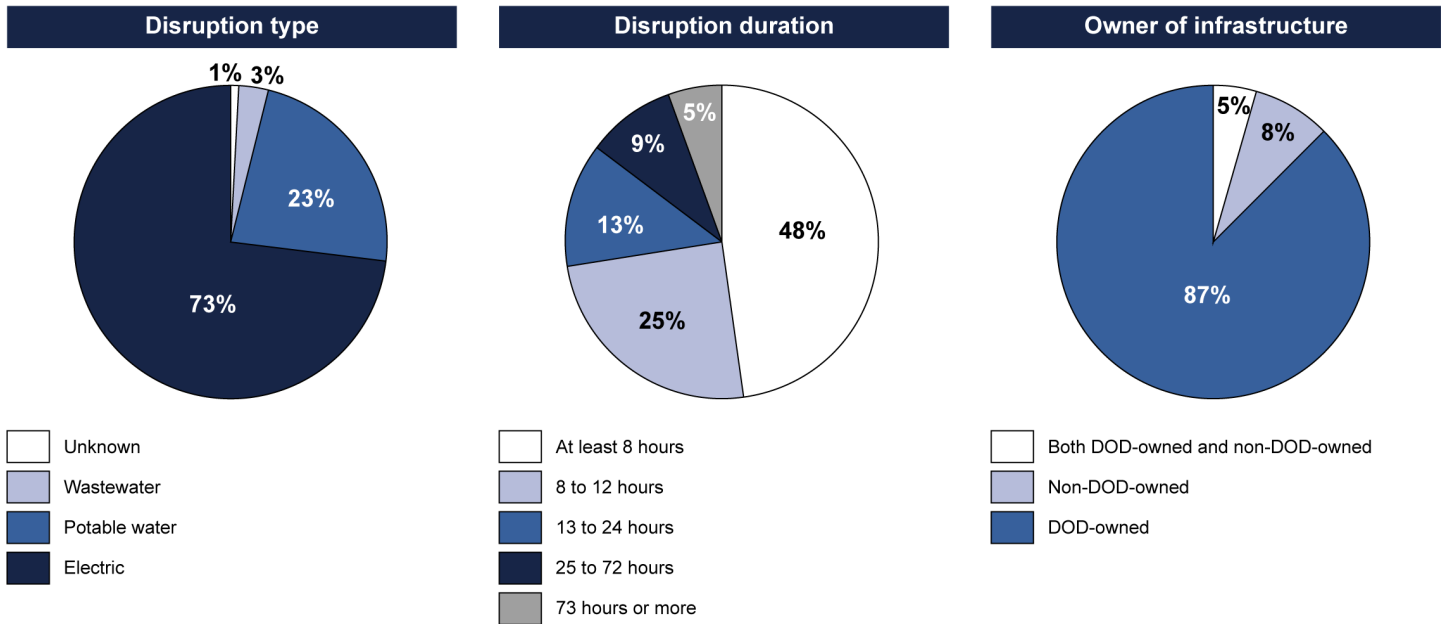
Figure 2: Number of Utility Disruptions Reported by DOD Components to the Office of the Secretary of Defense (OSD), Fiscal Years 2012 through 2014



Source: GAO analysis of Department of Defense (DOD) information. | GAO-15-749

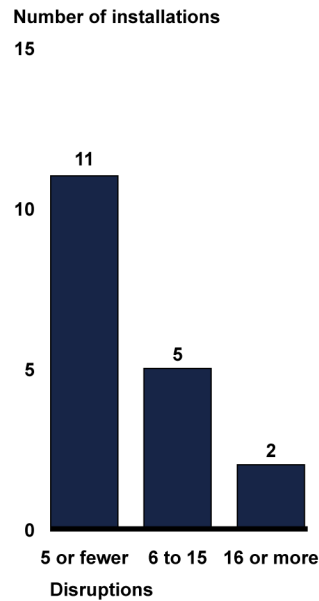
DOD’s Energy reports do not discuss specific examples of utility disruptions and their impacts on installation operations, in part because the statute does not require such examples. Thus, we decided to gather additional information on DOD utility disruptions from 20 installations we selected inside and outside of the continental United States, caused by hazards. As reflected in the figures below, from fiscal year 2012 to fiscal year 2014, utility disruptions on installations in our sample varied in their frequency, duration, the type of utility service disrupted, and the ownership of the utility infrastructure affected. Figures 3 and 4 summarize information on disruptions lasting 8 hours or longer, occurring in fiscal years 2012 through 2014, and reported to us by 18 of the 20 installations in our sample. Of these 20, 18 reported a total of 150 disruptions lasting 8 hours or longer that occurred in fiscal years 2012, 2013, or 2014. Figure 3 provides information on the type and duration of utility disruptions, and the owner of the utility infrastructure involved in the disruption. Figure 4 provides information on the number of disruptions experienced by installations in our sample.

Figure 3: Information on Disruptions Lasting 8 Hours or Longer, Fiscal Years 2012 through 2104, Reported to GAO by 18 DOD Installations inside and outside the Continental United States



Source: GAO analysis of Department of Defense (DOD) information. | GAO-15-749

Figure 4: Information on the Number of Disruptions Experienced by 18 DOD Installations inside and outside the Continental United States That Reported to GAO on Disruptions Lasting 8 Hours or Longer, from Fiscal Year 2012 through Fiscal Year 2014



Source: GAO analysis of Department of Defense (DOD) information. | GAO-15-749

Hazards Have Caused Utility Disruptions, with Operational and Fiscal Impacts, and Threats Have the Potential to Cause Such Impacts

Utility disruptions caused by hazards, such as mechanical failure and extreme weather events, have resulted in a number of serious operational and fiscal impacts. Further, both DOD and GAO have noted that climate change increases the likelihood of such events and the department must be prepared for—and have the ability to recover from—utility disruptions that impact mission assurance on its installations. According to officials from the 20 installations we visited or contacted, examples of utility disruptions’ impacts on installations’ operations include the following:

- In July 2013, two unusually strong thunderstorms downed power lines at Naval Air Weapons Station China Lake, California, causing electrical disruptions of 12 and 20 hours. The installation’s missions include supporting the Navy’s Research, Development, Acquisition, Test and Evaluation mission and providing Navy training capability. Because of these disruptions, the installation lost the ability to conduct 17 mission-related events, including 4 test events and 13 maintenance or training flights.

-
- In October through December of 2010 and June of 2013, Vandenberg Air Force Base experienced electrical disruptions due to mechanical failures, resulting in several impacts on installation operations. For example, these disruptions led to key systems being unavailable for space launch operations. Specifically, the disruptions contributed to delaying the launch of one satellite by about 5 days and another by 1 day. In addition, the installation has experienced wildfires. Figure 5 shows fire-damaged utility infrastructure on Vandenberg Air Force Base.

Figure 5: Utility Pole Damaged by a Wildfire on Vandenberg Air Force Base



Source: U.S. Air Force. | GAO-15-749

- In our May 2014 report on DOD's adaptation to climate change for infrastructure, we found operational impacts of climate change on installations' utility resilience.²⁷ For example, according to DOD officials, the combination of thawing permafrost, decreasing sea ice, and rising sea level on the Alaskan coast have led to an increase in coastal erosion at several Air Force radar early warning and communication installations. Installation officials explained that this

²⁷ [GAO-14-446](#).

erosion has damaged a variety of installation infrastructure, including utilities.

According to our review of information provided by officials from the 20 installations we visited or contacted, the fiscal impact of utility disruptions can vary. Examples of fiscal impact include the following:

- In late October and early November of 2012, storm surge from Hurricane Sandy destroyed potable water and wastewater utility infrastructure of a pier at Naval Weapons Station Earle, New Jersey. This damage resulted in a disruption of potable water and wastewater services to docked ships. Disruption of these utility services lasted about 1 month until—according to installation officials—the installation could contract to provide temporary potable water and wastewater services, with a variety of costs for the government. For example, according to an installation official, one contract to provide temporary utility service totaled about \$2.8 million. Also, according to Navy documentation, the Navy has estimated that more than \$23 million will be required to replace the destroyed infrastructure. Vandenberg Air Force Base has also experienced disruptions of potable water utility service. For example, a November 2014 disruption of water used by a power plant that provides electricity to a launch pad had an estimated repair cost of \$15,000. Figure 6 shows the repair of damaged potable water infrastructure on Vandenberg Air Force Base.

Figure 6: Repairs to a Potable-Water Pipe on Vandenberg Air Force Base



Source: U.S. Air Force. | GAO-15-749

-
- During unusually cold temperatures in January 2014, the utility company that provides natural gas service to the Army's Aberdeen Proving Ground, Maryland, implemented a curtailment agreement with the installation. Such agreements allow the utility provider to reduce service during periods of unusually high demand. However, due to mechanical failures, several of the installation's heating boilers were unable to switch from using natural gas to using fuel oil. As result, the installation was not able to curtail its purchase of natural gas, and was fined almost \$2 million by the utility provider.
 - In our May 2014 report on DOD's adaptation to climate change for infrastructure, we also found fiscal impacts of climate change on installations' utility resilience.²⁸ For example, in 2013, Fort Irwin, California, experienced three power disruptions in a span of 45 days. Caused by extreme rain events that created flash flooding, each disruption lasted at least 24 hours. The disruptions limited the effectiveness of instrumentation used to track the training at the National Training Center and provide information used for after-action feedback. To increase future utility resilience, Fort Irwin requested more than \$11.5 million for 31 backup generators. In our May 2014 report, we noted that weather-related fiscal impacts on infrastructure may increase in their frequency or severity due to climate change. If so, DOD's maintenance costs for these weather-related fiscal impacts are likely to increase.

Physical and cyber threats also have the potential to cause utility disruptions with impacts on installation operations. According to DOD officials, while there are no known malicious physical acts that have caused utility disruptions on DOD installations lasting 8 hours or longer, such acts have the potential to cause utility disruptions, with resultant impacts on installation operations. For example, according to the Federal Bureau of Investigation and the Pacific Gas & Electric utility company, in April 2013 an individual or individuals cut fiber optic cables and fired over 100 bullets into 13 large transformers located at a California substation operated by the company, damaging the transformers. According to DOD officials, this incident did not result in disruption of electrical service at DOD installations. However, they explained that the incident is an example of the type of utility disruption threat posed by physical terrorism.

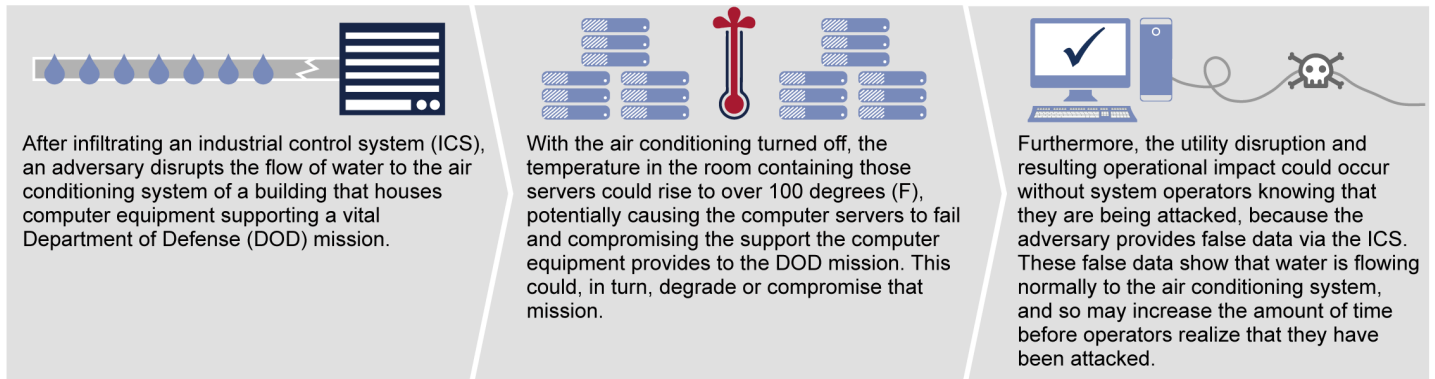
²⁸[GAO-14-446](#).

In addition, based on our review of DOD documents and discussions with DOD officials, the department's utility infrastructure is also under cyber threat. According to DOD's April 2015 Cyber Strategy, the global proliferation of malicious code or software, called "malware," increases the risk to U.S. networks and data. A variety of adversaries can purchase destructive malware and other capabilities on the black market. As cyber capabilities become more readily available over time, DOD assesses that state and nonstate actors will continue to seek and develop cyber capabilities to use against U.S. interests. Further, according to the March 2014 OSD memorandum discussed previously,²⁹ DOD's computer networks and systems—including ICS—are under "incessant" cyber attack and damage to or compromise of any ICS may be a mission disabler. For example, according to a briefing provided by an official from the United States Cyber Command, an adversary could gain unauthorized access to ICS networks and attack DOD in a variety of ways.

United States Cyber Command officials explained that there are several categories of cyber threats involving a DOD installation's ICS that have the potential to cause utility disruptions and resulting impacts on installation operations. The first category of cyber threats includes the removal of data from an ICS or a DOD network connected to an ICS. According to OSD's March 2014 memorandum, a serious mission-disabling event could occur if an ICS was used as a gateway into an installation's information technology system or possibly DOD's broader information networks. The second category of cyber threats involves the insertion of false data to corrupt the monitoring and control of utility infrastructure through an ICS. In its March 2014 memorandum, OSD noted that disruption of a computerized chiller controller could deleteriously impact critical military operations and readiness. Figure 7 details an example of a potential cyber attack provided by Navy officials.

²⁹Memorandum from the Acting Deputy Under Secretary of Defense for Installations and Environment, Subject: *Real Property-related Industrial Control System Cybersecurity*.

Figure 7: Example of a Potential Cyber Attack Using False Data in an Industrial Control System



Source: GAO analysis of DOD information. | GAO-15-749

The third category of cyber threats is the physical destruction of utility infrastructure controlled by an ICS. According to United States Cyber Command officials, this threat—also known as a “cyber-physical effect”—is the threat about which they are most concerned. This is because a cyber-physical incident could result in a loss of utility service or the catastrophic destruction of utility infrastructure, such as an explosion. According to one of the officials, an example of a successful cyber-physical attack through ICS was the Stuxnet computer virus that was used to attack Iranian centrifuges in 2010. Through an ICS, the centrifuges were made to operate incorrectly, causing extensive damage.

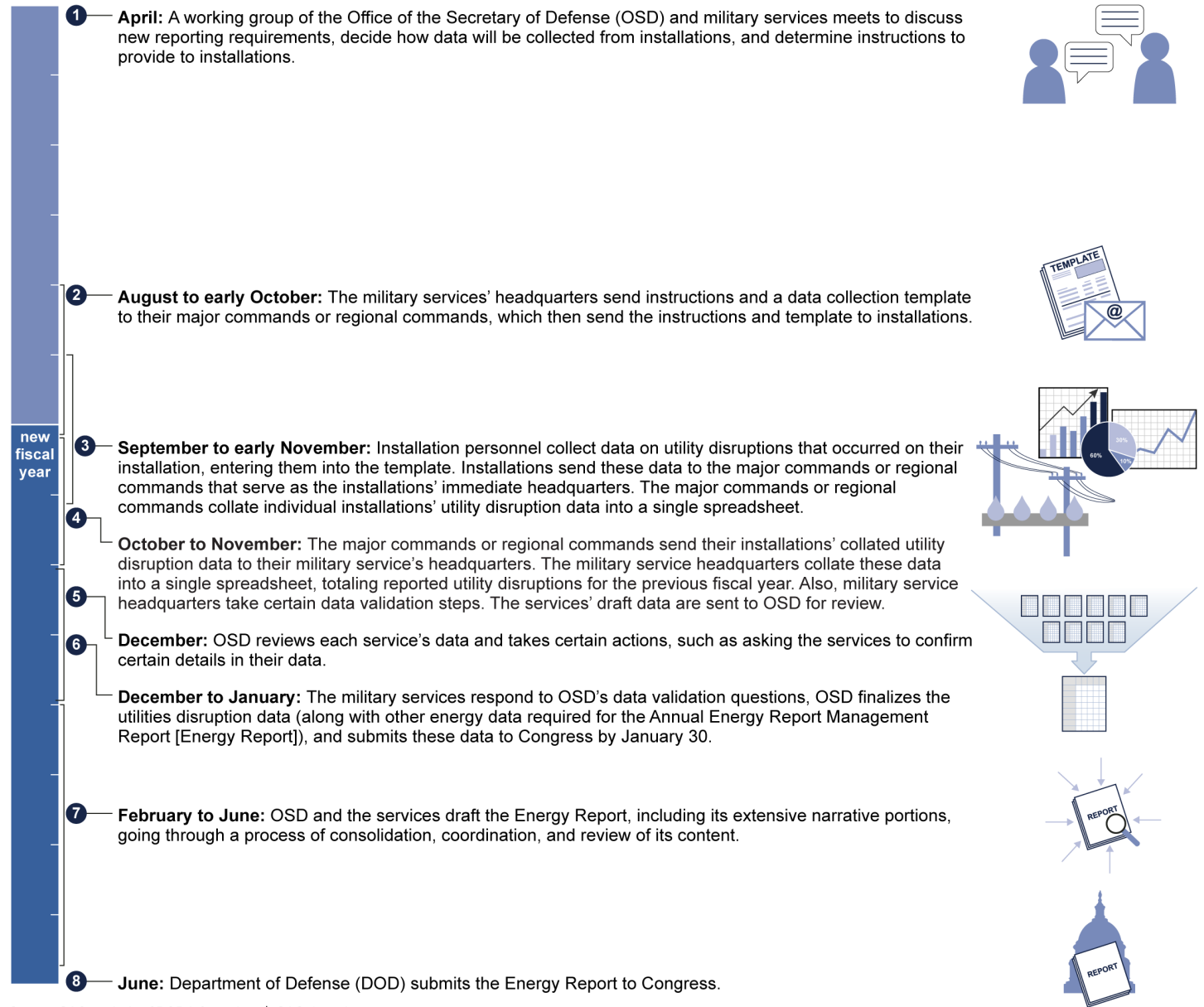
DOD Collects and Reports Utility Disruption Data, but Its Data Are Not Comprehensive and Some Are Not Accurate

DOD has a 5-month process to collect and report on utility disruption data, and uses these data in a number of ways. However, the department’s collection and reporting of utilities disruption data are not comprehensive and some data are not accurate.

DOD Has a 5-Month Process to Collect and Report on Utility Disruption Data, and Uses These Data in a Number of Ways

DOD undergoes an annual process to report on utility disruptions in its Energy Reports, collecting data required by Section 2925 of Title 10 of the United States Code—including utility disruption data—for the reports, over a 5 month time period. The overall process, with participation by installations, military service headquarters, and OSD, is detailed in figure 8.

Figure 8: DOD's Typical Process for Collecting the Data on Utility Disruptions Reported in Its Annual Energy Management Report



Source: GAO analysis of DOD information. | GAO-15-749

According to our review of the June 2013 and June 2014 Energy Reports, other DOD documents, and discussions with an OSD official responsible for planning and implementing utility resilience activities, DOD uses the utility disruption data in a number of ways. First, DOD has analyzed these data to support a review of existing DOD guidance on power resilience at DOD installations that is presently informing the department's policy.³⁰ Second, according to an OSD official, DOD can use the utilities disruption data as a baseline to establish trends that inform future strategic planning and policymaking. Further, the official explained that these are the only utility disruption data collected for the Energy Reports, and so are especially important to informing DOD's utility resilience efforts, noting that it is important for OSD decision making to be driven by analyzing data. Also, the official explained that analyses of the utility disruptions' average duration could inform decisions about which type of backup power infrastructure is the most cost-effective to install on installations. For example, if the average duration of a disruption is 2 to 3 days, individual generators may be the most cost-effective option. In contrast, if the average duration of a disruption is 7 days or longer, natural gas-powered plants located on installations may be the most cost-effective option. Third, DOD uses the utility disruption data collected from its installations to meet the requirement in Section 2925 of Title 10 of the United States Code to report to Congress on—among other things—the total number and location of utility outages on installations, their financial impact, and mitigation measures.

DOD's Collection and Reporting of Utilities Disruption Data Are Not Comprehensive and Some Data Are Not Accurate

DOD instructions in a template used to collect utility disruption data from installations stipulate that installations should report on external, commercial utility disruptions lasting at least 8 hours. According to officials from the military service headquarters and OSD, they do not review installations' utilities disruption data to determine whether there are instances that meet the reporting criteria but are not included. Officials from three of the military service headquarters and OSD³¹ stated that, in fiscal years 2012 through 2014, there were installations that did

³⁰The effort is discussed in more detail later in this report.

³¹In a discussion with us, Marine Corps headquarters officials stated that they do not know whether Marine Corps installations underreported. However, in our research, we determined that the Marine Corps did underreport.

not report on all disruptions that meet these criteria.³² By comparing the utility disruptions we identified through our independent research to those submitted by the military services to OSD,³³ we confirmed cases of underreporting by installations from all four services, although our comparative analysis does not quantify the extent of underreporting. For example, in fiscal years 2012 and 2013, the Army did not report at least four disruptions, including a 1-week potable water main break at Camp Darby, Italy.³⁴ Also, in fiscal year 2012 the Navy and Marine Corps did not report at least eight disruptions, seven of which were multiday electrical disruptions that occurred as a result of the June 2012 derecho storm, including a disruption at Marine Corps Base Quantico.³⁵ Thus, for fiscal year 2012, the number of the Navy and Marine Corps' unreported disruptions is at least more than double the number of reported disruptions. In addition, for fiscal years 2013 and 2014, the Navy and Marine Corps did not report a total of at least four disruptions.³⁶

Further, according to instructions in the data collection template, installations are supposed to submit data only on external, commercial

³²Neither DOD nor GAO is able to determine the total number of underreported disruptions. Because there is no source of information on all disruptions that meet DOD's criteria, there is no baseline to which we can compare the installations' submissions for fiscal years 2012 through 2014. For this reason, we conducted research into utility disruptions; our research was independent of the disruptions reported by the installations. To identify underreporting of disruptions, we compared the results of our research to the installations' submissions. For more information on our research methodology, see app. I.

³³This research consisted of identifying news articles and information from DOD websites and press releases on DOD utility disruptions that occurred beginning in 2005 and then having military services officials verify this information and identify which instances lasted 8 hours or more.

³⁴The other three disruptions we learned about were a multiday wastewater disruption at Fort Shafter and two electrical disruptions at Aberdeen Proving Ground.

³⁵A derecho is a combination of thunderstorms and strong winds. See GAO, *Climate Change: Energy Infrastructure Risks and Adaptation Efforts*, [GAO-14-74](#) (Washington, D.C.: Jan. 31, 2014). At least seven Marine Corps and Navy installations experienced disruptions as a result of the derecho storm. They are Marine Corps Base, Quantico, Virginia; Naval Air Station, Patuxent River, Maryland; Navy Information Operations Command, Sugar Grove, West Virginia; Naval Support Activity, Annapolis, Maryland; Naval Support Activity, Bethesda, Maryland; Naval Support Activity, South Potomac, Virginia; and Naval Support Facility / National Maritime Intelligence Center, Suitland, Maryland.

³⁶The four disruptions we learned about were at Naval Weapons Station Earle, Naval Air Weapons Station China Lake, Guam, and Camp Pendleton.

utility disruptions, not those associated with DOD-owned utility infrastructure, such as the mechanical failure of a DOD-owned transformer or a potable water pipe bursting. This results in underreporting of disruptions in DOD's Energy Reports. As noted above, at the 20 installations we visited or contacted, more than 90 percent of disruptions involved DOD-owned infrastructure. Specifically, for fiscal years 2012 to 2014, installations in our sample experienced almost 140 utility disruptions involving DOD infrastructure, which would not be captured in the Energy Reports. According to officials from multiple installations we visited or contacted, aging DOD-owned utility infrastructure contributes to utility disruptions. For instance, Kadena Air Force Base officials explained that "failing" DOD-owned utility infrastructure creates challenges to maintaining support to the installation's mission. The officials provided one example, noting that some wastewater pipes were cast in 1947 and have been in use for over 65 years. Kadena Air Force Base officials told us that, from 2011 to 2014, the installation experienced at least 40 disruptions of electrical, potable water, and wastewater utility services stemming from DOD-owned infrastructure that officials estimate lasted at least 8 hours.³⁷

DOD instructions in the data collection template also stipulate that installations should submit costs related to mitigating utility disruptions, such as the cost of generators or fuel on which generators run. In fiscal years 2012, 2013, and 2014, three of the four military services submitted disruption data to OSD that did not include information on mitigation costs. For 194 of those disruptions—or 48 percent of the 404 utility disruptions reported to OSD for that period—installations did not report mitigation costs. Because it is common for DOD installations to have backup generators that provide power during electrical disruptions—and an OSD official stated that the majority of reported disruptions are electrical—it is likely that installations reporting electrical disruptions also experienced costs associated with generators. For instance, Navy officials noted that almost every Navy installation has at least some generators that would run during a disruption and these generators

³⁷ According to Officials from Kadena Air Force Base, they were able to provide the actual duration for six of the disruptions. For the remaining disruptions, the officials could not provide the actual duration, due to limitations in their record-keeping capabilities. Therefore, the officials used 40 man-hours of repair work as a metric to estimate which disruptions exceeded 8 hrs. This is because, according to the officials, most extended utility outages require a work crew of four to five personnel to correct.

consume fuel that would need to be replaced at a cost. Thus, it is likely that DOD underreported certain costs associated with disruptions such as fuel costs for generators.

In addition to underreporting, our review of the fiscal years 2012 through 2014 utilities disruption data submitted by the military services to OSD and discussions with OSD officials show there were inaccuracies in duration and cost data on disruptions reported in DOD's June 2013 and June 2014 Energy Reports. In regard to the duration of disruptions, three of the four military services included disruptions lasting less than 8 hours in the data they submitted to OSD. In total, the military services submitted 32 disruptions lasting less than 8 hours for fiscal years 2012 through 2014.³⁸ However, according to an OSD official, the fiscal year 2012 and 2013 disruptions lasting less than 8 hours were included in the data reported in the June 2013 and June 2014 Energy reports, constituting about 12 percent of the 266 disruptions DOD reported.³⁹ Further, for fiscal years 2012 and 2013, a total of 104 disruptions were submitted with incomplete information on duration.⁴⁰ Specifically, these disruptions lacked start and end times. According to our analysis of Air Force disruptions reported to OSD for fiscal year 2012 and OSD information on the number of Air Force disruptions reported in the June 2013 Energy Report, it is likely that the disruptions were included in the data reported in that report. Further, according to OSD officials, the Army disruptions were included in the data reported in the June 2014 Energy Report. The 104 disruptions without complete information on duration account for almost 40 percent of the 266 disruptions that DOD reported for fiscal years 2012 and 2013.

There were also inaccuracies regarding the cost of disruptions. As discussed above, DOD instructions in the data collection template stipulate that installations should submit direct costs related to mitigating utility disruptions, such as the cost of generators or fuel for them. The instructions also stipulate that indirect costs related to utility disruptions, such as an installation's lost productivity, should not be submitted. For fiscal year 2012, the Army submitted costs related to the disruption of

³⁸The Army submitted 1; the Navy 21; and the Air Force 10.

³⁹As of May 2015, DOD had not issued its June 2015 Energy Report containing fiscal year 2014 utility disruption data.

⁴⁰16 disruptions were submitted by the Air Force and 88 were submitted by the Army.

electrical utility service at Fort Belvoir, Virginia, as a result of the June 2012 derecho storm. According to the Army's descriptions of these submissions, a total of \$4.63 million was for indirect costs, specifically: lost sales, spoiled inventory (e.g., food, medicine), or lost productivity. However, according to OSD officials, these costs were included in the data reported in the June 2013 Energy Report. This \$4.63 million of inaccurately reported indirect costs accounts for 66 percent of the approximately \$7 million in total costs reported by DOD for fiscal year 2012.

Based on our review of the fiscal year 2014 data submitted by the military services to OSD—and OSD's data validation efforts—the accuracy of DOD's data may be improving. For example, based on our review, the services' fiscal year 2014 data contained some inaccuracies, but there were fewer duration and cost inaccuracies than in the fiscal year 2013 data. Also, OSD's data validation documentation show OSD removed several inaccurate military service submissions before providing the final fiscal year 2014 data set to the Congress. However, challenges remain in the data collection instructions DOD provides to its installations and in the department's review and validation of data, which could hinder consistent improvement over time.

According to the Standards for Internal Control in the Federal Government, program managers need operational and financial information in order to determine whether they are meeting their agencies' plans and goals, and to promote the effective and efficient use of resources.⁴¹ Also, in previous work examining how DOD was meeting reporting requirements, we found that complete and accurate data are key to meeting such requirements.⁴² In addition, in previous work examining—among other things—DOD's efforts to effectively implement existing guidance, we found that clear and complete guidance is important to the effective implementation of responsibilities.⁴³ The standards also emphasize the importance of accurately recording events. Further, according to the standards, managers should continually assess their processes to ensure the processes are updated as necessary. In

⁴¹[GAO/AIMD-00-21.3.1](#).

⁴²[GAO-14-777](#).

⁴³[GAO-14-446](#).

addition, according to the Project Management Institute's 2013 guide to project management, standard practices in program management include—among other things—reviewing a process on a regular basis to recommend changes or updates to the process.⁴⁴

DOD's underreporting of some disruptions that met the criteria laid out in DOD reporting instructions, and not including disruptions of DOD-owned utility infrastructure in the Energy Reports, are likely due to two factors related to instructions in DOD's data collection template for installations. First, the underreporting of disruptions that meet DOD's criteria is likely due to inconsistent guidance provided to installations. Specifically, headquarters officials from both the Marine Corps and Air Force stated that they provided verbal guidance to their installations to submit disruptions only if the disruptions met service-specific criteria different than those stipulated in DOD's data collection template. For example, Air Force headquarters officials explained that, for collection of data for fiscal year 2014, they instructed their installations to submit disruptions only if they were not mitigated by back-up utility infrastructure, such as an electrical disruption mitigated by a generator. However, the data collection template does not instruct installations to limit their submissions based on these criteria. Also, based on our review, DOD's instructions to installations place inconsistent emphasis on electrical and nonelectrical utilities and provide an unclear scope of the data to be submitted. For instance, the instructions begin by listing the electrical, water, and gas utilities on which the installation is supposed to report, but the instructions' details refer only to disruptions in electrical power. Officials from several installations we visited found these instructions confusing. For example, officials from two of the installations stated that they did not submit information on potable water disruptions due to the confusing nature of the instructions.

Second, the instructions in the data collection template stipulate that installations are to submit only external, commercial disruptions because—according to an OSD official—DOD decided to limit the scope of data collection and reporting to external, commercial disruptions. The official explained that when the statutory requirement to collect data on utility disruptions began in fiscal year 2012, DOD's rationale was that

⁴⁴Project Management Institute, *A Guide to the Project Management Body of Knowledge*.

almost all of the electricity used by its installations is provided by non-DOD entities such as external, commercial utility companies.

As discussed above, the military service headquarters and OSD take various steps to validate utility disruption data submitted by the installations and military services, respectively, but the time and rigor they commit to reviewing the disruption data are limited, which could affect their comprehensiveness and accuracy. Specifically, according to officials from both the military service headquarters and OSD, the structure of the current process for collecting and reporting data in the Energy Reports gives relatively little time to validate the utilities disruption data. DOD officials explained that, out of the 5-month process for collecting and reporting these data, there are 3–4 weeks in which they review utility disruption data. Also, officials from certain military service headquarters explained that their review of installations' data looks for clear "outliers" or data that seem incorrect and that they rely on installations to provide accurate data on instances of commercial external utility disruptions and associated mitigation costs. In addition, OSD spends about 2 weeks reviewing all of the data required for the Energy Report, including the disruption data. OSD's validation efforts include questions for the military services that address individual items submitted by each service. According to an OSD official, the 2 weeks it has allotted to review all of the Energy Report's data means that it is difficult to verify installation-level information.

An OSD official and certain headquarters officials also explained that—in their limited time to validate all of the data included in the Energy Reports—they prioritize validation of other data types above their review of the utilities disruption data. These other types of data represent the 11 other categories of data that DOD is required to include in the Energy Report. According to certain military services headquarters officials, they prioritize validation of other data types above their review of the utilities disruption data because they feel OSD places a higher priority on other data, such as those related to DOD requirements or renewable energy projects. In our review of OSD's data validation of the military services' fiscal years 2013 and 2014 data for the Energy Reports, we found that a

large majority of the questions are about types of data other than utilities disruption data.⁴⁵

Without more comprehensive and accurate collection and reporting of utilities disruption data in DOD's Energy Reports, the department and Congress face a number of risks. First, the underreporting of external, commercial utility disruptions and not reporting on disruptions caused by DOD-owned infrastructure mean that DOD's Energy Reports run the risk of not providing a full picture of utility disruptions on DOD installations. GAO's research and analysis indicates that DOD-owned infrastructure may play a larger role in disruptions than indicated by the Energy Reports, which only address external, commercial disruptions.⁴⁶ For example, as discussed previously in this report, the installations we visited or contacted reported almost 140 disruptions involving DOD infrastructure, some with significant impacts, such as delayed satellite launches at Vandenberg Air Force Base or almost \$26 million in estimated repair costs at Naval Weapons Station Earle. By not including disruptions to DOD-owned infrastructure, the Energy Reports understate costs and impacts. Second, in regard to reported disruptions, potential underreporting of certain costs associated with disruptions and inaccuracies in the reporting of disruptions' duration and cost mean that DOD's Energy Reports run the risk of misrepresenting two key impacts of disruptions. For example, the average duration of disruptions reported in the June 2014 Energy Report could misrepresent the actual average duration of fiscal year 2013 disruptions, given that DOD did not include the duration for more than 50 percent of these disruptions. Also, because of potential underreporting of certain costs associated with disruptions, both the June 2013 and June 2014 reports may not fully capture the costs associated with mitigating electrical disruptions. In addition, the total cost reported in the June 2013 Energy report likely misrepresents the actual type of cost data on disruptions that the military services were instructed

⁴⁵We were unable to review OSD's validation of the military services' fiscal year 2012 data because OSD was not able to provide these data validation questions. According to an OSD official, these documents were lost during an OSD transition from an older computer system to the office's current computer system. However, he explained that these technical challenges have now been resolved.

⁴⁶As we discussed previously, our sample of 20 installations is nongeneralizable, and so we cannot assume that this trend applies to the universe of DOD's installations. However, the research conducted on these installations provides valuable insight for our study. For more information on our research methodology, see appendix I.

to report, given that 66 percent of the costs DOD included were indirect costs. Because DOD used these data to support an existing utility resilience initiative and may use the data to inform future planning and policymaking, accurate data are especially important to informing DOD's utility resilience efforts. Third, the limited collection and reporting of utilities disruption data in DOD's Energy Reports may hamper congressional oversight of DOD utility resilience actions.

The Military Services Have Taken Actions and Implemented DOD Guidance to Mitigate Risks of Utility Disruptions but Face Challenges in Implementing Cybersecurity Guidance for Industrial Control Systems

The military services have taken actions and implemented a number of different pieces of DOD guidance to mitigate the risk of utility disruptions. In addition the military services have begun planning for the implementation of DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT),⁴⁷ to generally mitigate the risk of cyber incidents on all DOD information technology systems and ICS, but face challenges in implementing this guidance for ICS.⁴⁸

⁴⁷DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)* (Mar. 12, 2014).

⁴⁸DOD's Risk Management Framework, DOD Instruction 8510.01, is based on the National Institute of Standards and Technology's series of information security standards and guidelines developed by the Joint Task Force Transformation Initiative Interagency Working Group with representatives from the civil, defense and intelligence communities, which started an effort in fiscal year 2009 to produce a unified information security framework for the federal government. The joint task force's working group members include representatives from DOD, the National Institute of Standards and Technology, and others. The series' flagship document is Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. Other publications in the series include Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. DOD Instruction 8510.01 references several of these publications.

Military Services Have Taken Actions and Implemented DOD Guidance to Mitigate Utility Disruptions

Based on our review of DOD documents, and according to officials from installations both inside and outside the continental United States that we visited or contacted, installations have taken various actions to mitigate the effects of disruptions in electrical, potable water, wastewater, and natural gas utility service.

- 19 of the 20 installations we visited or contacted use backup generators to provide emergency power to certain facilities. For example, Marine Corps Base Camp Pendleton has about 158 facilities with active emergency generators that it utilizes during electrical disruptions. Further, the installation has identified a prioritized order for refueling, the goal of which is to keep the generators operating during emergency situations.
- At the locations we visited or contacted, installations have taken a number of actions to mitigate risk to potable water and wastewater utility service. For instance, at Wheeler Army Airfield, Hawaii, officials explained that—in the event of an electrical disruption disabling potable water pumps—the installation’s potable water system is fed by water tanks, and certain pump stations have emergency generators. In addition, Vandenberg Air Force Base has a sewage pond that can store up to 3 days’ worth of sewage in the event that the pipes leading to the treatment facility cannot be used. Installations have also developed contingency plans for access to potable water resources in addition to their primary source. Further, certain installations have upgraded their utility infrastructure in order to improve its resilience. According to Naval Weapons Station Earle officials, the potable and wastewater infrastructure, destroyed by Hurricane Sandy, is designed to be stronger and thus more resilient in the face of future extreme storms. Figure 9 shows both the damaged and repaired infrastructure.

Figure 9: Potable and Wastewater Infrastructure at Naval Weapons Station Earle Destroyed by Hurricane Sandy, and New, Strengthened Water Lines Being Installed



Destroyed by Hurricane Sandy



New, strengthened water lines being installed

Source: U.S. Navy. | GAO-15-749

In addition, installations in our sample have taken steps to plan for emergency situations in which utility service could be disrupted. For example, the Naval Base San Diego, California, emergency management plan has an appendix that addresses potential disruptions in electrical, potable water, and wastewater utility service; includes planned response actions; and lists installation organizations responsible for certain actions. Also, according to officials at Tengan Pier and White Beach in Japan, both installations participate in emergency management exercises that provide them with the opportunity to focus on various utility disruption scenarios, such as an exercise that features a typhoon scenario. Finally, Joint Base Pearl Harbor-Hickam, Hawaii, has an emergency management plan that identifies all emergency resources available at the installation such as portable generators, portable pumps, generators providing power to other utilities (water production facilities, wastewater treatment plant, and lift stations), and information on emergency capabilities and assessment teams.

The installations in our sample also are generally taking steps in response to DOD guidance related to utility resilience and have taken steps to mitigate the risk to installations posed by utility disruptions

caused by both threats and hazards.⁴⁹ According to military service headquarters officials, there are several pieces of DOD-wide guidance related to utility resilience. Table 1 summarizes selected DOD guidance and our analysis of implementation efforts by installations in our sample. Examples of actions taken by installations to implement this guidance follow the table.

Table 1: Selected DOD Guidance Related to Mitigating Risk to Operations at Installations in the Event of Utility Disruptions and Summary of Our Analysis of Implementation Efforts by Installations in Our Sample

DOD guidance	Description	Implementation efforts by installations in our sample
Defense Energy Program Policy Memorandum 92-1	States that it is the basic responsibility of defense managers and commanders to know the vulnerability of their missions and installations to energy disruptions, whether the energy source is internal or external to the command.	19 of the 20 installations have taken steps to implement this guidance, such as preparing emergency response plans or conducting vulnerability assessments.
Department of Defense (DOD) Instruction 2000.16, DOD Antiterrorism (AT) Standards (Oct. 2, 2006, incorporating change Dec. 8, 2006)	Focuses on protecting—among other things—DOD installations and infrastructure critical to mission accomplishment from terrorist attack.	20 installations have taken steps to implement this guidance, such as conducting various assessments that examine the threat of a terrorist attack.
DOD Instruction 4170.11, Installation Energy Management (Dec. 11, 2009)	Requires installations to conduct vulnerability assessments of basic mission requirements to energy disruptions, and—among other things—implement remedial actions to remove unacceptable energy supply risk.	19 of 20 installations have taken steps to implement this guidance, such as assessing vulnerabilities and the condition of utility systems.
DOD Directive 3020.40, DOD Policy and Responsibilities for Critical Infrastructure (Jan. 14, 2010, incorporating change Sept. 21, 2012) ^a	Provides guidance for the Defense Critical Infrastructure Program and assigns related roles and responsibilities.	Some installations have been involved in a Defense Critical Infrastructure Program assessment. ^b

Source: GAO analysis of DOD data.

^aAccording to DOD officials, the department is increasing its ability to assess vulnerabilities to critical infrastructure by integrating existing vulnerability assessments under one program, the Mission Assurance Assessment Program. According to DOD's April 2015 Cyber Strategy, currently, DOD components take varying approaches to measuring and assessing cyber risks for mission assurance. Specifically regarding utility services, the integrated assessments will address topics such as the current electrical power system's ability to meet current and future demands and the presence of redundant electrical feeds to the installation.

^bNot every DOD installation has defense critical infrastructure; thus not every installation would be involved in a Defense Critical Infrastructure Program assessment.

⁴⁹Specifically, we asked each installation we visited or contacted about any efforts related to the requirements in the selected guidance documents as listed in table 1. Our intent was to assess the extent to which these installations were taking actions to implement the utility resilience measures contained in the selected guidance found in table 1.

Based on our review of DOD documents and discussions with officials at military service headquarters and installations, implementation efforts include actions such as preparing emergency response plans, conducting vulnerability assessments, and assessing the condition of utility infrastructure. For example, Aberdeen Proving Ground's emergency response plan identifies utility system vulnerabilities, emergency preparedness requirements, and remedial actions intended to mitigate the risk of potential utility service disruptions. Officials from several locations stated that their installations had undergone various assessments of the vulnerability of utility infrastructure to terrorist attack. Furthermore, officials from Naval Base San Diego and Naval Air Weapons Station China Lake stated that they were conducting a utility inventory and risk assessment, which would assess and rate the condition of the utility and also document the consequences of failure of utility infrastructure.

In addition to mitigation actions and implementation of guidance taken at the installation level, DOD has undertaken a number of department-wide initiatives to enhance utility resilience. For example, in 2013, the Assistant Secretary of Defense for Energy, Installations and Environment directed a review of existing DOD guidance on power resilience at DOD installations.⁵⁰ While reliable and continuous access to all types of utilities is important to DOD missions, OSD officials stated that they focused this review on power because other utility services may depend on—and many DOD missions specifically rely on—reliable access to power. Officials from the Office of the Assistant Secretary of Defense for Energy, Installations and Environment are currently reviewing the responses from the DOD installations, which were compiled and submitted by each military service, and developing recommendations for power resilience requirements.

In addition, DOD has taken—or participated in—efforts to enhance department-wide cybersecurity of ICS. For instance, the United States Cyber Command and the Joint Test and Evaluation Program—under the Director, Operational Test and Evaluation, Office of the Secretary of Defense—initiated a collaborative effort in 2014 to develop a set of procedures to detect, mitigate, and respond to cyber incidents on DOD

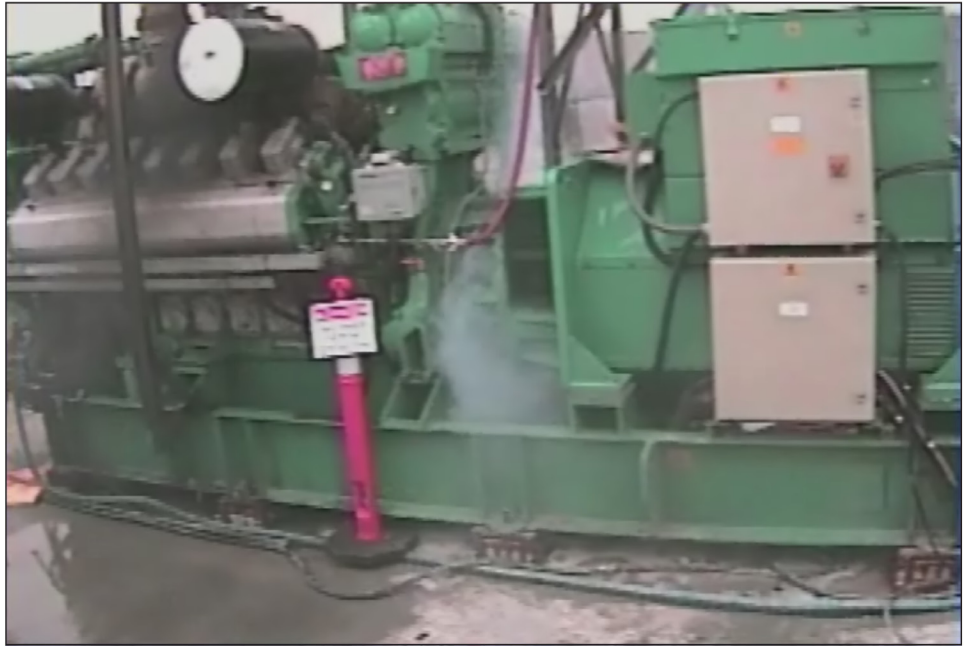
⁵⁰According to DOD's definition, power resilience is the planning and capability to ensure the department has available, reliable, and high-quality power to continuously accomplish missions from its installations in the face of potential disruptions. For the purposes of this report, power resilience is a type of utility resilience.

ICS perpetrated by advanced persistent threat actors, such as nation states. These procedures are intended to be employed by DOD installation personnel such as installation information technology managers and ICS facility engineers. An official from the command stated that the draft procedures will be tested at a joint exercise in June 2015 and expects the procedures to be completed by December 2015.⁵¹

Also, according to our review of documents from the Department of Homeland Security and DOD—and discussions with officials from both agencies—DOD has undertaken efforts to better understand cyber threats to ICS that monitor and control DOD utility infrastructure on which DOD relies. In one example of such efforts, the Idaho National Laboratory—under the direction of the Department of Homeland Security and with participation from DOD—conducted the Aurora Test in 2007. This test demonstrated how catastrophic physical damage can be caused to utility infrastructure—in this case a diesel generator—from a remote location through an adversary’s exploitation of vulnerabilities in the ICS used to monitor and control electrical substations. After the test, the diesel generator was inspected and it was determined that it would not be capable of operation without extensive repairs or a complete overhaul. While not all generators are configured in the fashion of the Aurora Test, U.S. Cyber Command officials stated that the Aurora Test is applicable to DOD generators since some have the same equipment as discussed in the Aurora Test and that cyber methods can be used to misconfigure how this equipment operates causing damage or destruction to the equipment. Figure 10 shows a still photo from a video of the Aurora test.

⁵¹The exercise, Cyber Guard, is an annual joint cyberspace training exercise sponsored by U.S. Cyber Command. Multiple agencies participate in the exercise, including the Department of Homeland Security.

Figure 10: Video Still Photo Showing Physical Damage to Generator during Cyber Attack Test by Idaho National Laboratory



Source: Department of Homeland Security. | GAO-15-749

Note: to view the full video, please click on the video hyperlink <http://www.gao.gov/products/GAO-15-749>.

DOD Updated
Cybersecurity Guidance
for Industrial Control
Systems, and the Military
Services Have Taken
Initial Steps to Implement
the Guidance

In addition to the guidance mentioned previously, DOD has developed guidance that addresses utility resilience with respect to the cybersecurity of ICS that control and monitor utility systems, and the military services have begun planning for its implementation.

In March 2014, the department issued DOD Instruction 8510.01,⁵² which establishes the policy for a risk management framework for all DOD information technology, including ICS.⁵³ DOD Instruction 8510.01 replaces the previous DOD policy for information assurance, the DOD Information Assurance Certification and Accreditation Process, which primarily addressed security related to information technology systems.⁵⁴ According to officials, the former accreditation process required that the communication connection between an ICS and a DOD communication network be accredited. However, it did not require ICS to be certified and accredited. DOD officials stated it would be very rare for any organization to have conducted an assessment of the cyber vulnerabilities of an ICS system on a DOD installation because—before DOD’s adoption of DOD Instruction 8510.01—ICS had not been a focus of security assessments. For example, according to a Navy and Marine Corps document,⁵⁵

⁵²DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT) (Mar. 12, 2014).

⁵³DOD Instruction 8510.01 uses the term “platform information technology systems” to categorize the types of systems that include utility ICS. DOD defines these systems as a collection of information technology hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, and that is structured by physical proximity or by function. Examples of platform information technology systems include weapons, training simulators, medical technologies, buildings and their associated control systems (such as building automation systems or building management systems, and energy management systems), utility distribution systems (such as electric, water, wastewater, and natural gas), telecommunications systems designed specifically for ICS to include supervisory control and data acquisition, direct digital control, programmable logic controllers, and other control devices and advanced metering. Because utility infrastructure and systems are the focus of this report, we are using the term “ICS” rather than “platform information technology systems.”

⁵⁴DOD Instruction 8510.01 reissued and renamed the former instruction with the same number called *DoD Information Assurance Certification and Accreditation Process* (Nov. 28, 2007).

⁵⁵Navy Facilities Engineering Command, *Navy and Marine Corps Smart Grid: Capability Development Document* (Washington, D.C.).

currently most Navy and Marine Corps ICS have very little in the way of security controls and cybersecurity measures in place.⁵⁶

According to a March 2014 DOD memorandum, for the first time DOD is now requiring that ICS be made secure against cyber attacks by implementing the Risk Management Framework.⁵⁷ To mitigate cybersecurity threats to ICS—discussed earlier in this report—DOD Instruction 8510.01 directs the DOD Chief Information Officer and the heads of each DOD component to oversee the implementation of the instruction.⁵⁸ In addition, DOD Instruction 8510.01 states that DOD component heads must complete tasks such as, among others, conducting an impact-based categorization of existing ICS, assigning qualified personnel to risk management framework roles, and identifying and programming funding for the implementation in budget requests. According to DOD, by implementing DOD Instruction 8510.01, the military services will be able to identify vulnerabilities, adopt cybersecurity controls, and mitigate risks of cyber incidents on ICS that could cause potentially serious utility disruptions.

According to military service headquarters officials, the services have begun planning for and have taken some actions toward implementation of DOD Instruction 8510.01.

- Headquarters officials stated that each of the military services has a working group that is examining how to implement DOD Instruction 8510.01. For example, Army officials stated that they have formed a planning team, composed of officials with expertise in cybersecurity, information technology, and ICS, that is examining how the Army will implement DOD Instruction 8510.01.
- In addition, military service officials stated that they plan to revise current service-level ICS cybersecurity policies to align with DOD

⁵⁶According to DOD's April 2015 Cyber Strategy, DOD's own network is a patchwork of thousands of networks across the globe, and DOD lacks the visibility and organizational structure required to defend its diffuse networks effectively.

⁵⁷Memorandum from the Acting Deputy Under Secretary of Defense for Installations and Environment, Subject: *Real Property-related Industrial Control System Cybersecurity* (Mar. 19, 2014).

⁵⁸The DOD Chief Information Officer is responsible for matters concerning DOD information technology and cybersecurity. See DOD Directive 5144.02, *DOD Chief Information Officer (DOD CIO)* (Nov. 21, 2014).

Instruction 8510.01. Air Force, Navy, and Marine Corps officials stated that they have policies that assess the cybersecurity of ICS, but that the policies do not cover the requirements in DOD Instruction 8510.01. In addition, Navy headquarters officials stated that they issued draft guidance in February 2015, which, according to these officials, outlines the Navy's process for accreditation of ICS cybersecurity per requirements in DOD Instruction 8510.01.

- Navy, Marine Corps, and Air Force officials stated that they are developing technical capabilities that will assist with the implementation of DOD Instruction 8510.01. For example, Air Force officials are developing a concept called ICSNet, which includes hardware and software designed to monitor ICS operations and provide intrusion-detection capabilities. Further, OSD officials stated that they are refining the Enterprise Mission Assurance Support Service tool, which manages certification and accreditation processes for DOD Instruction 8510.01, to better support ICS-specific requirements.

The Military Services Face Challenges Implementing Cybersecurity Guidance for Industrial Control Systems

The military services face three challenges—conducting an inventory of existing ICS; finding qualified personnel with the necessary skills to implement the cybersecurity requirements; and identifying funding needed to implement DOD Instruction 8510.01—related to their implementation of cybersecurity guidance for ICS. According to military service officials, the services have not yet implemented DOD Instruction 8510.01 and transitioning to the instruction is a complex and difficult task. Evidence of this difficulty is that—according to officials from the office of the DOD Chief Information Officer—DOD revised the original time frames to transition to DOD Instruction 8510.01 because they were unachievable. Specifically, the original time frames required the military services to transition ICS without a current accreditation to DOD Instruction 8510.01 by September 2014, among other things. DOD's adjusted time frames allow the services until the second quarter of fiscal year 2018 to implement DOD Instruction 8510.01. According to Army officials, the adjusted time frames will allow the military services additional time to plan for the transition. However, even with the additional time, the services may be challenged to implement DOD Instruction 8510.01.

Military service headquarters officials stated that they are still developing an inventory of their services' respective ICS. DOD Instruction 8510.01 requires that ICS should be categorized based on the potential impact on an organization. As part of this categorization, it is necessary to inventory the ICS and collect information about the system, such as the type of information collected and maintained on the system and technical aspects

of the system, such as the type of operating system used. Military officials we spoke with explained that an inventory of ICS is an important tool for managing the various types and locations of ICS on military installations. Navy officials explained that a complete inventory of ICS would help headquarters officials communicate information about updated security vulnerabilities to system owners.

However, as of February 2015, none of the military services had a complete inventory of existing ICS. While each service is taking steps to obtain a complete inventory, the data collection process is challenging. For example, the Air Force is planning on issuing a data call to its installations in May 2015 and expects that the process will take 6 months to complete. Currently, Air Force officials stated that they are aware of 280 ICS across the Air Force and estimate that the total number of systems on active-duty Air Force bases is around 1,900. Marine Corps officials stated that they also issued a data call to their installations to collect information on the numbers and types of ICS, but the information that they received was only 80 percent complete. Marine Corps officials explained there are challenges that impeded their ability to collect the information. For example, officials stated that the management of ICS at the installation level is decentralized such that no one individual has visibility over all of the ICS on the installation. Navy officials stated they have an ICS inventory of about 18,000, which includes about 37,000 buildings. Officials stated that obtaining a complete list may be challenging without the authority to address all organizations on Navy installations. In addition, they stated that some tenants on Navy-operated installations do not wish to share information about their ICS. However, if the ICS owned by another service on a joint base—or by a tenant on Navy base—is connected to a Navy network, it may be a cybersecurity risk to the Navy installation. Also, Navy officials stated that it is still unclear which organizations on Navy bases have the responsibility for these types of ICS, and that the Navy will need to overcome these challenges if it is to have a complete ICS inventory.

Furthermore, officials from each military service stated that identifying personnel with the appropriate expertise will be a challenge due to a shortage of personnel with experience in both the operation and maintenance of ICS and in cybersecurity. DOD Instruction 8510.01 states that qualified personnel should be assigned to risk management framework roles. According to United States Cyber Command and military services headquarters officials, there are very few personnel that have both the cybersecurity technical skills and the skills regarding the operation and maintenance of ICS. Specifically, the Navy does not have

the personnel with expertise to determine the necessary cybersecurity controls for each ICS or to maintain the cybersecurity controls for the ICS once they are in place. Air Force officials stated that the most important issue related to implementation of DOD Instruction 8510.01 for ICS at the installation level is the lack of a qualified staff member assigned the responsibility for ICS cybersecurity. Moreover, officials also identified a lack of available training to provide personnel with the necessary skills. For example, Army and Navy officials stated that the DOD training and certification classes currently available are specific to information technology systems such as desktop computers, and not to ICS. The Marine Corps has begun providing training to a limited number of personnel, but had to use training provided by the Department of Homeland Security's Industrial Control System Cyber Emergency Response Team. Department of Homeland Security officials stated that they have limited capacity and are not funded or staffed to support the training needs of DOD.

Military service headquarters officials also stated there are several funding-related challenges to implement DOD Instruction 8510.01, including that implementation may require significant resources and costs involved in implementation have not been fully identified. DOD Instruction 8510.01 states that it is DOD policy that resources for implementing the DOD Risk Management Framework must be identified and allocated as part of the Defense planning, programming, budgeting, and execution process. For example, a required aspect of implementation is identifying resources to remediate or mitigate vulnerabilities discovered through the assessment process.

- According to some estimates provided by the military service headquarters officials, implementing DOD Instruction 8510.01 for ICS will require substantial resources. For example, Navy officials estimated that the Navy will need “billions of dollars” to secure ICS over what they characterized as the long term, 10 to 20 years, which involves developing a standardized approach that helps protect ICS and implementing updates to systems so that the systems are operating within current cybersecurity standards.⁵⁹ According to the officials, this cost figure also includes all of the necessary training

⁵⁹In addition, in the short term, Navy officials estimated that they will need approximately \$60 million to secure ICS. This cost involves examining the Navy's current ICS and installing updates so that current ICS are operating with current cybersecurity standards.

involved and the creation of new positions. In addition, Marine Corps headquarters officials estimate that the cost to implement DOD Instruction 8510.01 could range between \$3.8 million to \$4.2 million per year for the “first few years” of implementation.⁶⁰ The officials stated that these costs include funding to develop the technical capability that is being developed in partnership with the Navy and hiring contractor support to assess ICS against the cybersecurity standards.

- Further, military service headquarters officials explained that the military services have not yet programmed funding for implementation. For example, Army officials stated that they anticipate including \$2.5 million in the fiscal year 2017-2021 budget request to be used in fiscal year 2017 to conduct an inventory of ICS, however budget decisions have not yet been made for these budget years. Further, no funding is programmed for fiscal years 2015 and 2016. Navy officials stated that some tasks related to ICS cybersecurity have been funded using existing funds. For example, funds from the Navy Facilities Engineering Command’s working capital fund were used to pay for some ICS cybersecurity assessments. However, the Navy has not yet specifically programmed funds to implement DOD Instruction 8510.01.
- In addition, military service officials stated that they have not fully identified the costs involved in implementing DOD Instruction 8510.01 and face challenges in identifying those costs. For example, Army and Marine Corps officials stated that it is difficult to develop an accurate estimate of resources needed to support the implementation of DOD Instruction 8510.01 without a complete inventory and prioritization of ICS, which is not yet complete. Specifically, Marine Corps officials stated that while they have developed an estimate, it is still just their “best guess” based on available information. Furthermore, Air Force officials explained that one of the elements of the overall cost to implement DOD Instruction 8510.01 depends on the costs associated with the technical capability the Air Force is developing in order to implement DOD Instruction 8510.01. However, officials explained that they are still in the early stages of developing the capability and have not fully identified the costs. Without knowing the costs, officials explained that they cannot estimate the overall costs to implement DOD Instruction 8510.01.

⁶⁰In addition, after the implementation of DOD Instruction 8510.01 is under way, Marine Corps officials estimated that the costs of maintaining the program would go down to about \$2.9 million to \$3 million per year.

Challenges with conducting an inventory of existing systems, identifying individuals with the necessary expertise, and programming and identifying funding to implement DOD Instruction 8510.01 may hamper the military services' abilities to plan for and execute the implementation of DOD Instruction 8510.01 by the March 2018 time frame. For example, if the Air Force's inventory is not completed until November 2015, it only has 28 months to transition an estimated 1,900 ICS to DOD Instruction 8510.01, which means that almost 70 ICS would need to be accredited each month to meet DOD's time frames. In addition, given that there are three remaining fiscal years until DOD's fiscal year 2018 deadline for fully transitioning to DOD Instruction 8510.01, the fact that the military services have not programmed for or fully identified transition costs means that the services may be at risk of not adequately funding key transition tasks. According to DOD's April 2015 Cyber Strategy, because DOD's capabilities cannot necessarily guarantee that every cyberattack will be denied successfully, the department must invest in resilient and redundant systems so that it may continue operations in the face of disruptive or destructive cyberattacks on DOD networks. Until DOD Instruction 8510.01 is implemented, DOD installations' ICS remain vulnerable to exploitation because of a lack of cybersecurity controls. Vulnerabilities in ICS can be exploited by various methods causing loss of data, denial of service, or the physical destruction of infrastructure.⁶¹ For instance, as previously discussed, Stuxnet is an example of a computer worm, a method of cyberattack that can target ICS vulnerabilities. In 2010, Stuxnet targeted ICS used to manage centrifuges in an Iranian nuclear processing facility. According to DOD, the same type of ICS can be found in the critical infrastructure on numerous DOD installations. Without overcoming challenges related to completing inventories, acquiring and training personnel, and identifying and programming for funding, all of which are required under DOD Instruction 8510.01, the military services' ICS may be vulnerable to cyber incidents that could degrade operations and negatively impact missions.

⁶¹According to the Department of Homeland Security, common vulnerabilities in ICS include weak passwords or no policies to enforce the use of strong passwords, the lack of network segmentation and poorly configured firewalls, and no documented security policies and procedures. See, Department of Homeland Security, *Common Cybersecurity Vulnerabilities in Industrial Control Systems* (Washington, D.C.: May 2011).

Conclusions

To support its operational missions, DOD depends on reliable access to electrical, potable water, wastewater, and natural gas utility services on its installations. As events of the past few years have demonstrated, this access can be disrupted by hazards such as extreme weather and mechanical failures. These extreme weather events may be further exacerbated by the impacts of climate change. In addition, as we and DOD have noted, utilities are vulnerable to threats from physical and cyber terrorism. Given the possibility of disruptions that result in serious operational impacts, decision makers in DOD and Congress need reliable information on the actual scope of disruptions in order to exercise oversight and ensure that resources are available to take necessary steps at installations and across the department to increase resilience. Without guidance that clarifies the reporting requirements of installations—including the need to fully report on all types of disruptions, including disruptions of nonelectrical utilities—and requires the inclusion of disruptions to DOD-owned utilities, decision makers may lack a comprehensive understanding of the types of utility disruptions on DOD installations. In addition, DOD and the military services have the opportunity to take steps that could improve the comprehensiveness and accuracy of the data they collect, such as assessing the effectiveness of the current 5-month data collection process. Data that are more complete and accurate are important, especially given that DOD has stated that the utility disruption data it collects have been used to support ongoing and future plans for resiliency initiatives. As our report indicates, installations have taken steps to mitigate the impacts of disruptions and increase resilience, with infrastructure that provides redundancy and through the implementation of utility resiliency guidance. However, DOD and the military services face several challenges in supporting the department's effort to implement its Risk Management Framework for ICS. We recognize that DOD is in the early stages of this effort and that it plans on full implementation. Full implementation is important, since cyber attacks on ICS can lead to the loss of operational data and disruption of utility service. As previously discussed, we have identified long-standing challenges with the government's cybersecurity efforts. Without taking steps now to conduct an inventory of existing ICS, identify individuals with the expertise needed to implement DOD Instruction 8510.01, and program and identify resources for implementation, the military services risk future delays in their efforts to plan and execute the steps necessary to protect installation infrastructure from utility disruptions that could have direct operational mission impacts.

Recommendations for Executive Action

In order to provide DOD and Congress with more comprehensive and accurate information on all types of utility disruptions, we recommend that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force; the Commandant of the Marine Corps; and the Assistant Secretary of Defense for Energy, Installations and Environment to take the following two actions to provide more consistent guidance to the installations:

- First, in guidance provided to their installations, the military services should clearly state that all disruptions lasting 8 hours or longer should be reported, regardless of the disruptions' impact or mitigation. In addition, the military services and OSD should work together to revise the data collection template's instructions, clarifying that disruptions in all four categories of utility service—electrical, potable water, wastewater, and natural gas—should be reported.
- Second, the military services and OSD should revise the data collection template's instructions to include reporting of disruptions caused by DOD-owned utility infrastructure.

Also, in order to improve the comprehensiveness and accuracy of certain data submitted by the military services to OSD and reported in the Energy Reports—such as potentially underreported data on mitigation costs and inaccurate data on both disruptions' duration and cost—we recommend that the Secretary of Defense direct the Secretaries of Army, Navy, and Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations and Environment to work together to improve the effectiveness of data validation steps in DOD's process for collecting and reporting utilities disruption data. For example, the military services and OSD could determine whether more time in the 5-month process should be devoted to data validation and whether equal priority should be given to validating all types of data included in the Energy Reports.

Further, in order to minimize the risk of delays in their efforts to implement DOD Instruction 8510.01, we recommend that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force; and the Commandant of the Marine Corps to address challenges related to inventorying existing ICS, identifying personnel with the appropriate expertise, and programming and identifying funding, as necessary.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD and the Department of Homeland Security for review and comment; both departments provided technical comments that we considered and incorporated as appropriate. DOD provided written comments on our recommendations, which are reprinted in appendix III.⁶²

In its written comments, DOD partially concurred with our first two recommendations (now combined as one recommendation), concurred with two recommendations, and non-concurred with one recommendation. DOD also stated that it did not agree with GAO's analysis of the comprehensiveness and accuracy of the department's reporting on utility disruptions in the June 2013 and 2014 Energy Reports. However, as discussed in this report, DOD's collection and reporting of utilities disruption data are not comprehensive and some data are not accurate. For instance, in regard to comprehensiveness, we confirmed cases of installations in each military service that did not report on the commercial, external disruptions on which they are directed to report by DOD reporting guidance. Also, in regard to accuracy, there were inaccuracies in duration and cost data on disruptions reported by DOD. For example, more than 100 disruptions without complete information on duration account for almost 40 percent of the disruptions that DOD reported in the June 2013 and 2014 Energy Reports.

Our first recommendation—aimed at providing DOD and Congress with more comprehensive and accurate information on all types of utility disruptions—originally appeared as two recommendations in the draft report provided to DOD for comment. Based on that draft, DOD partially concurred, asking us to consider combining the two recommendations, because they both impact DOD guidance. DOD's suggested combination of our first and second recommendations—as written in the department's response—meets the intent of the original two recommendations. Thus, we have combined them into one recommendation, and in subsequent conversations with DOD, an OSD official confirmed that the department concurs with the combined recommendation. DOD's written responses did not provide information on the timeline or specific actions it plans to take to implement our recommendations.

⁶²DOD's agency comment letter refers to GAO-15-547SU, a non-public version of this report, GAO-15-749. While the non-public version contains an appendix with sensitive information, the same recommendations are included in both reports. Thus, DOD's comments in its letter pertain to both versions, GAO-15-547SU and GAO-15-749.

In regard to our recommendation originally appearing third—that OSD and the military services revise the data collection template’s instructions to include reporting of disruptions caused by DOD-owned infrastructure—DOD did not concur. The department stated that reporting on these disruptions provides a “low value proposition;” the data collected by the department for the Energy Reports is not being used to guide its strategic decisions; and collecting the data would be “onerous.” We disagree that collecting data on utility disruptions caused by DOD-owned infrastructure would be of low value. As discussed in the report, our research indicates that DOD-owned infrastructure, which DOD controls, may play a larger role in disruptions than indicated by the Energy Reports, which only address external, commercial disruptions involving equipment over which DOD has little control. For example, the installations we visited or contacted reported disruptions involving DOD infrastructure with significant impacts, such as delayed satellite launches at Vandenberg Air Force Base and almost \$26 million in estimated repair costs at Naval Weapons Station Earle. In addition, DOD stated that the data we collected on utility disruptions caused by DOD-owned infrastructure only confirm trends in the data on external, commercial disruptions already collected by DOD. However, we continue to believe its Energy Reports may be missing a substantial number of disruptions by not including disruptions caused by DOD-owned infrastructure.⁶³ Our analysis found that more than 85 percent of utility disruptions in our sample involved DOD-owned infrastructure on which DOD does not report in the Energy Reports. Further, the department stated that the utility disruption data it collects for the Energy Reports is not being used to guide strategic decisions. However, as previously discussed in our report, DOD has used utility disruption data collected for the Energy Reports to support a DOD-wide utility resilience initiative. This was a strategic-level decision, although based on limited information, since data on disruptions involving DOD-owned infrastructure were not collected for DOD’s annual reports. We believe that, if DOD takes actions to improve the comprehensiveness and accuracy of its utilities disruption data, the data could serve as a valuable tool in making additional well-informed utility resilience decisions. Collecting data on disruptions caused by DOD-owned infrastructure may give the department information on disruptions it has a greater ability to mitigate and DOD would have more complete

⁶³As discussed previously, in this study we report on data in way that parallels DOD’s data collection. Specifically, we report on utility disruptions lasting eight hours or longer that occurred in fiscal years 2012 to 2014.

information on which to make any future strategic decisions, such as the resiliency initiative discussed above. And, by collecting and reporting data on utility disruptions caused by DOD-owned infrastructure, the department would be giving Congress a more complete picture of disruptions on DOD installations. Finally, DOD stated that collecting data on disruptions caused by DOD-owned infrastructure would create an “onerous” reporting requirement that requires collection, review, and coordination across the department. However, DOD provided no evidence that collecting these additional data would be “onerous.” The installations we contacted were able to provide these data to us and DOD’s current data collection process already includes collection, review, and coordination across the department.

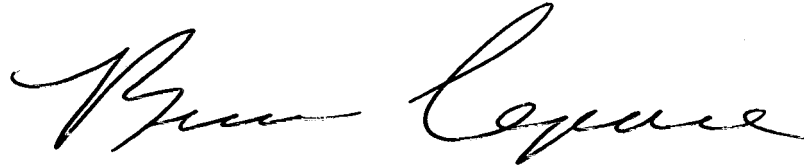
In regard to our recommendations originally appearing fourth and fifth—regarding improvements in DOD’s process for collecting and reporting utilities disruption data and addressing challenges in implementing DOD Instruction 8510.01, regarding ICS—DOD concurred. However, DOD did not provide information on the timeline or specific actions it plans to take to implement our recommendations.

DOD also requested that, in our recommendations, we remove references to the Marine Corps, because it is part of the Department of the Navy. In regard to the issues on which we made recommendations, the Marine Corps and Navy collaborate and take some shared actions, under the Department of the Navy. However, the Marine Corps and Navy also take actions that are specific to each military service. For example, the Marine Corps and Navy headquarters collect utilities disruption data from their installations through distinct processes and the two services have distinct plans for implementing DOD Instruction 8510.01. For this reason, we believe the recommendations are appropriately directed at the Marine Corps and Navy as separate military services.

We are providing copies to the appropriate congressional committees; the Secretaries of Defense, Homeland Security, the Army, the Navy, and the Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations, and Environment. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4523 or leporeb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last

page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink, appearing to read "Brian Lepore". The signature is fluid and cursive, with the first name "Brian" and the last name "Lepore" clearly distinguishable.

Brian J. Lepore
Director, Defense Capabilities and Management

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Thad Cochran
Chairman
The Honorable Richard J. Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Rodney Frelinghuysen
Chairman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

To determine whether threats and hazards have caused utility disruptions on Department of Defense (DOD) installations—and if so—what impacts they have had, we reviewed various types of documents on utility disruptions and resulting impacts on installation operations. Examples of documents we reviewed include DOD and Department of Homeland Security assessments of utilities' vulnerability to both hazards and threats, and DOD's June 2013 and June 2014 Annual Energy Management Reports (Energy Reports). In addition, we interviewed or contacted officials from a nongeneralizable sample of 20 DOD installations from inside and outside the continental United States. To identify the installations for our sample, we took a number of steps. First, we reviewed military service data submitted to the Office of the Secretary of Defense (OSD) on utility disruptions that occurred on DOD installations from fiscal years 2012 to 2014 and lasted 8 hours or longer. According to our analysis of information provided by an OSD official, the military services account for about 87 percent of the utility disruptions reported to OSD for fiscal years 2012 to 2014. Because their installations account for a large majority of reported disruptions, we focus on the military services' utility disruptions in this report. Because DOD's data in its Energy Reports do not provide specific examples of disruptions and their impacts, we conducted independent research using publicly available information, such as news articles, the details of which we then asked officials from the military services to verify. We collected additional data on utility disruptions from 2005 to 2014 on installations inside and outside the continental United States, in order to gather a large number of utility disruptions lasting 8 hours or longer, and their impacts.¹ Next, we reviewed the military services' data and the additional data we gathered, in order to select the 20 installations to include in our nongeneralizable sample. We selected installations based on whether the installations had more than one instance of utility disruption, or had a disruption of multiple types of utility service; and we chose installations from each military service. For installations inside the continental United States, we visited the sites, collected information in interviews, and gathered supporting documentation. For sites outside the continental United States, we collected written answers to the questions, along with supporting documentation. From the 20 installations, we gathered information on utility disruptions and their impacts; actions they had taken to mitigate

¹For the purposes of this report, we are defining *utility disruption* as an outage or interruption of service lasting eight hours or longer. This definition is used by DOD in its Energy Reports.

such impacts; and implementation of selected pieces of DOD utility resilience guidance, discussed in more detail below. As discussed above, the installations in our sample provided information on utility disruptions from 2005 to 2014, lasting 8 hours or longer. In our sample of 20 installations, 18 installations reported a total of 150 disruptions lasting 8 hours or longer that occurred in fiscal years 2012, 2013, or 2014; 2 installations reported disruptions lasting 8 hours or longer that occurred prior to fiscal year 2012.² Although the information we collected was not representative of all installations, the selection of these installations provided valuable insights for our review. In addition, we assessed the reliability of all computer-generated data provided by the installations in our sample by reviewing existing information about the data and the systems that produced the data and by interviewing agency officials knowledgeable about the data to determine the steps taken to ensure its completeness and accuracy. We determined that these data were sufficiently reliable for the purposes of presenting the number and certain characteristics of utility disruptions, as reported by officials from installations in our sample. However, as noted in our report, we determined those utilities disruption data reported by DOD in its June 2013 and June 2014 Energy Reports were not sufficiently reliable for the purpose of comprehensively or accurately presenting the total number, average duration, or cost of utility disruptions. Table 2 lists the installations we visited or contacted and their locations.

Table 2: Installations Visited or Contacted

Installation	Location
Aberdeen Proving Ground	Maryland
Fort Shafter	Hawaii
Joint Base McGuire-Dix-Lakehurst	New Jersey
Joint Base Pearl Harbor-Hickam	Hawaii
Joint Region Marianas	Guam
Kadena Air Force Base	Japan
Marine Corps Base Hawaii	Hawaii
Marine Corps Base Camp Pendleton	California

²Our sample consisted of the 20 installations listed in table 2 in this appendix. The installations in our sample provided information on utility disruptions from 2005 to 2014, lasting 8 hours or longer. Of these 20 installations, 18 installations reported a disruption lasting 8 hours or longer that occurred in fiscal years 2012, 2013, or 2014.

Installation	Location
Misawa Air Force Base	Japan
Naval Air Weapons Station China Lake	California
Naval Base San Diego	California
Naval Support Facility Diego Garcia	Diego Garcia
Naval Base Guam	Guam
Naval Weapons Station Earle	New Jersey
Naval Support Activity Andersen	Guam
Schofield Barracks	Hawaii
Tengan Pier	Japan
Vandenberg Air Force Base	California
Wheeler Army Airfield	Hawaii
White Beach Naval Facility	Japan

Source: GAO.

To determine the extent to which DOD’s collection and reporting of information on utility disruptions is comprehensive and accurate, we reviewed the statutory reporting requirement for the Energy Reports, compared the military services’ data submissions for fiscal years 2012 through 2014 with information we collected from the installations we visited or contacted, and reviewed DOD’s process for collecting and reporting on this data. DOD is statutorily required to report on—among other things—the total number and location of utility outages on installations. To respond to this requirement, the military services provide information to OSD. We reviewed the military services’ submissions of utility disruption data to OSD for fiscal years 2012 through 2014,³ as well as the June 2013 and June 2014 Energy Reports in which DOD reported these data. We reviewed these two reports because, at the time of our review, DOD had not yet issued its June 2015 report. To identify the comprehensiveness of DOD’s reporting, we compared the military services’ data submissions to OSD with the independent research we conducted at 20 installations in our sample, as described above. When comparing the data from our sample with the military service data submitted to DOD, we included only the 150 disruptions that occurred on the sample’s installations from fiscal years 2012 through 2014. In addition, we reviewed DOD instructions on the data submissions that provide information to the military services on the scope and type of

³This reporting requirement began in fiscal year 2012.

information the military services and their installations are supposed to submit to OSD. We then compared the services' submissions to DOD instructions for installations that provided these data. Our comparison covered the 3 years the military services submitted data for DOD's Energy Reports, fiscal years 2012 through 2014. Also, we reviewed documentation of OSD's validation of the military services' submissions. In addition, we met with officials at installations from our sample, the military services' headquarters, and OSD to discuss how utilities data were collected, validated, and reported. We also discussed the data validation processes used by officials at both the military services' headquarters and OSD. Further, to determine how DOD uses these utilities disruption data, we reviewed the June 2013 and June 2014 Energy Reports and met with officials at both the military services' headquarters and OSD. Finally, we compared DOD's processes for the collection, validation, reporting, and use of these data to several leading practices for the use and management of data and process improvement. Sources for these leading practices include the Standards for Internal Control in the Federal Government;⁴ our previous work that discusses improvement of infrastructure planning processes to better account for climate change impacts and improvement in the accuracy and completeness of data used to meet reporting requirements;⁵ and the Project Management Institute.⁶

To determine 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, we collected and reviewed DOD documents related to actions taken to mitigate risks, utility resilience guidance, and implementation efforts. We collected these documents from the 20 installations in our nongeneralizable sample and from the military service headquarters. To determine the extent to which DOD has

⁴GAO, *Auditing and Financial Management: Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

⁵GAO, *Climate Change Adaptation: DOD Can Improve Infrastructure Planning and Processes to Better Account for Potential Impacts*, [GAO-14-446](#) (Washington, D.C.: May 30, 2014); and *Depot Maintenance: Accurate and Complete Data Needed to Meet DOD's Core Capability Reporting Requirements*, [GAO-14-777](#) (Washington, D.C.: Sept. 18, 2014).

⁶Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, 5th ed. (2013). PMBOK is a trademark of Project Management Institute, Inc.

taken actions to mitigate risks to operations at its installations in the event of utility disruptions, we reviewed documents such as those describing backup generators on installations and the refueling plans for those generators. We also reviewed documents describing installations' plans for situations in which utility service is disrupted, to include emergency management plans. To determine DOD guidance related to utility resilience, we reviewed *Defense Energy Program Policy Memorandum 92-1*, DOD Instruction 2000.16, *DOD Antiterrorism (AT) Standards* (Oct. 2, 2006, incorporating change Dec. 8, 2006), DOD Instruction 4170.11, *Installation Energy Management* (Dec. 11, 2009), DOD Directive 3020.40, *DOD Policy and Responsibilities for Critical Infrastructure* (Jan. 14, 2010, incorporating change Sept. 21, 2012). In addition, we also reviewed documents related to the installations' implementation steps, such as vulnerability analyses that cover all threats and hazards. In addition, we met with officials from our sample of installations, and from military service headquarters to discuss actions taken to mitigate risks of utility disruptions, identify guidance related to utility resilience, and to identify steps taken to implement the guidance. Furthermore, we collected and reviewed DOD documents and guidance related to cybersecurity of industrial control systems (ICS), which are often used to monitor and control utility infrastructure on DOD installations.⁷ Specifically, we reviewed DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)* (Mar. 12, 2014). We reviewed documentation from OSD and the military services regarding cybersecurity of ICS, to include briefings and acquisition documents. We collected additional information from the Department of Homeland Security's Industrial Control System Cyber Emergency Response Team, to include documents describing common vulnerabilities of ICS. Also, we met with officials from the military services' and DOD's Offices of the Chief Information Officer, officials from the military services' headquarters offices, and OSD to discuss actions DOD had taken to begin implementation of DOD Instruction 8510.01 and challenges regarding implementation. Finally, we compared DOD's implementation actions to the implementation goals in DOD Instruction 8510.01.

⁷Industrial control systems (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as skid-mounted Programmable Logic Controllers often found in the industrial sectors and critical infrastructures, including utility systems.

We conducted this performance audit from June 2014 to July 2015, 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Previous GAO Work on the Vulnerabilities of Utility Infrastructure

Previous GAO work has examined the federal government's efforts to manage the physical security of the nation's critical infrastructure and the vulnerabilities of the systems that support critical infrastructure, including the commercial electric grid, to cyber attacks.

In October 2009, we reported that DOD's most critical assets are vulnerable to electrical power disruptions, but that DOD lacks sufficient information to determine the full extent of its vulnerability.¹ We recommended that DOD complete vulnerability assessments and develop guidelines for assessing the critical assets' vulnerabilities to long-term electrical power disruptions, among other things. In June 2011, DOD implemented this recommendation by updating guidance for the execution of vulnerability assessments and issued a timeline to ensure the accomplishment of tasks and to provide feedback to components on the status of actions, including electrical power-related risks and vulnerabilities.

Over the last decade, beginning in 2005, we have reported vulnerabilities in the protection of civilian critical infrastructure, including energy,² potable water,³ and wastewater.⁴ For example, in 2012, we found that the Department of Homeland Security, the agency responsible for implementing policies for the protection of civilian critical infrastructure, faced challenges in sharing the results of security surveys and vulnerability assessments with asset owners, to include those in the energy sector. Among other things, we recommended that the Department of Homeland Security develop a plan with time frames and milestones to ensure the timely delivery of the results of security surveys and vulnerability assessments to asset owners. In 2013, the Department of Homeland Security stated that it has implemented a web-based

¹GAO, *Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets*, [GAO-10-147](#) (Washington, D.C.: Oct. 23, 2009).

²GAO, *Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments*, [GAO-12-378](#) (Washington, D.C.: May 31, 2012).

³GAO, *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges*, [GAO-05-327](#) (Washington, D.C.: Mar. 4, 2005).

⁴GAO, *Securing Wastewater Facilities: Utilities Have Made Important Upgrades but Further Improvements to Key System Components May Be Limited by Costs and Other Constraints*, [GAO-06-390](#) (Washington, D.C.: Mar. 31, 2006).

approach to delivering this information to improve timeliness. Regarding potable water, in 2005, we found that community water systems faced obstacles in implementing security measures, including insufficient financial resources to implement security enhancements and determining how best to use available funds given competing priorities such as non-security-related infrastructure upgrades.⁵ We did not make any recommendations in this report. In regard to wastewater, we reported in 2006 that these facilities have made security improvements but they have been limited, and that additional coordination among the Environmental Protection Agency and Department of Homeland Security regarding initiatives to enhance wastewater facility security is needed.⁶ We recommended that these two agencies, among others, identify how to reduce overlap and duplication and how access to timely security threat information could be improved. The Environmental Protection Agency implemented this recommendation by updating the Water Information Sharing and Analysis Center, which improved access to timely and authoritative security threat information.

In January 2011, we also reported on the vulnerabilities of the systems that support critical infrastructure including the commercial electric grid to cyber attacks.⁷ Specifically, we identified several challenges to securing electricity systems and networks, including a lack of a coordinated approach to monitor industry compliance with voluntary standards, a focus by utilities on regulatory compliance instead of comprehensive security, and a lack of security features consistently built into systems. We made recommendations to the Federal Energy Regulatory Commission to address these challenges by periodically evaluating the

⁵In [GAO-05-327](#), we define “community water systems” as public water systems that supply water to the same population year round and the primary focus of critical infrastructure efforts in the water sector.

⁶The Environmental Protection Agency’s overarching mission is to protect human health and the environment by implementing and enforcing the laws intended to improve the quality of the nation’s air, water, and lands. The Department of Homeland Security has five core missions to prevent terrorism and enhance security; secure and manage our borders; enforce and administer our immigration laws; safeguard and secure cyberspace; and, ensure resilience to disasters.

⁷GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed*, [GAO-11-117](#) (Washington, D.C.: Jan. 12, 2011). Additionally, we have issued a number of reports on the cybersecurity of the nation’s critical infrastructure. Please see the Related GAO Products page for other reports.

extent to which utilities are following voluntary cybersecurity standards and developing strategies for addressing any gaps in compliance with these standards, among other things.⁸ While the Federal Energy Regulatory Commission agreed with these recommendations, they have not yet been implemented.

Additionally, in December 2014 we reported that federal facilities' industrial control systems (ICS)⁹ are vulnerable to cyber attacks.¹⁰ Specifically, we reported that these ICS—used to control things such as heating, ventilation, air conditioning, and electronic card readers—are increasingly being connected to the Internet and their vulnerability to potential cyber attacks is also increasing. We found that the Department of Homeland Security had not developed a strategy that defines the problem; roles and responsibilities; necessary funds; and a methodology for assessing the cyber risk. We recommended that the Department of Homeland Security develop a strategy with these components to address the cyber risk to these ICS. The department concurred with this recommendation and stated that it will develop a strategy.

⁸The Federal Energy Regulatory Commission is an independent federal agency that regulates the interstate transmission of electricity, natural gas, and oil, and oversees the reliability of high-voltage interstate transmission systems, among other responsibilities.

⁹Industrial control systems (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations such as skid-mounted Programmable Logic Controllers often found in the industrial sectors and critical infrastructures, including utility systems.

¹⁰GAO, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*, [GAO-15-6](#) (Washington, D.C.: Dec. 12, 2014).

Appendix III: Comments from the Department of Defense



ENERGY,
INSTALLATIONS
AND ENVIRONMENT

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

3400 DEFENSE PENTAGON
WASHINGTON, DC 20301-3400

JUN 26 2015

Mr. Brian J. Lepore
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Lepore:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-15-547, "DEFENSE INFRASTRUCTURE: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning," dated May 28, 2015 (GAO Code 351943). Detailed comments on the report recommendations are enclosed.

Sincerely,

A handwritten signature in black ink, appearing to read "John Conger".

John Conger
Performing the Duties of the Assistant Secretary of Defense
(Energy, Installations and Environment)

Enclosure:
As stated

GAO Draft Report Dated May 28, 2015
GAO-15-547 (GAO CODE 351943)

**“DEFENSE INFRASTRUCTURE: IMPROVEMENTS IN DOD REPORTING AND
CYBERSECURITY IMPLEMENTATION NEEDED TO ENHANCE UTILITY
RESILIENCE PLANNING”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

DoD does not agree with GAO’s analysis on the comprehensiveness and accuracy of reporting. Therefore, DoD has provided GAO multiple technical comments to address issues in GAO’s analysis. The technical comments have been provided for publication with the report.

For all recommendations, DoD requests consideration that references to “the Commandant of the Marine Corps” be removed. The Marine Corps is part of the Department of the Navy.

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the secretaries of the Army, Navy, and Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations and Environment take action to provide more consistent guidance to the installations. In guidance provided to their installations, the military services should clearly state that all disruptions lasting 8 hours or longer should be reported, regardless of the disruption’s impact or mitigation.

DoD RESPONSE: Partially concur. Please see next response.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct the secretaries of the Army, Navy, and Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations and Environment take action to provide more consistent guidance to the installations. The military services and OSD should work together to revise the data collection template’s instructions, clarifying that disruptions in all four categories of utility service-electrical, potable water, waste water, and natural gas-should be reported.

DoD RESPONSE: Partially concur. DoD requests consideration to combine Recommendation 1 and 2 since they both impact guidance. The combination of the two recommendations will allow for the more efficient implementation of guidance across the DoD. The new recommendation could read as follows:

“The GAO recommends that the Secretary of Defense direct the secretaries of the Army, Navy, and Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations and Environment take action to provide more consistent guidance to the installations. In guidance and procedures provided to their installations, OSD and the military services should clearly state that all disruptions lasting 8 hours or longer should be reported,

regardless of the disruption's impact, mitigation or utility service type (e.g., electric, potable water, waste water, and natural gas)."

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense direct the secretaries of the Army, Navy, and Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations and Environment take action to provide more consistent guidance to the installations. The military services and OSD should revise the data collection template's instructions to include reporting of disruptions caused by DOD-owned utility infrastructure.

DoD RESPONSE: Non-concur. As stated in DoD's technical comments to GAO, this recommendation provides a low value proposition. It will create an onerous reporting requirement which requires collection, review, and coordination across the DoD. The study findings indicate this data would not change the strategic results that utility outages are predominantly electric, of short duration, and not caused by physical or cyber events.

Further, since the data is not being used to guide strategic decisions and is better suited to guide local decisions, a better recommendation may be to require this data to be maintained at the Service or installation-level. OSD can provide oversight by including this language in current guidance and also direct targeted audits as the data is needed. For example, if a major event occurs, OSD can request the causes of the outages and share lessons learned with Congressional leaders for those installations impacted.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense direct the secretaries of the Army, Navy, and Air Force, the Commandant of the Marine Corps, and the Assistant Secretary of Defense for Energy, Installations and Environment to work together to improve the effectiveness of data validation steps in DOD's process for collecting and reporting utilities disruption data.

DoD RESPONSE: Concur.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense direct the secretaries of the Army, Navy, and Air Force, and the Commandant of the Marine Corps to address challenges related to inventorying existing ICS, identifying personnel with the appropriate expertise, and programming and identifying funding, as necessary.

DoD RESPONSE: Concur.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Brian J. Lepore, (202) 512-4523 or leporeb@gao.gov

Staff Acknowledgments

In addition to the contact named above, Laura Durland, Assistant Director; Ben Atwater; Hilary Benedict;Carolynn Cavanagh; Peter Haderlein; Karl Maschino; Steven Putansu; Jeanett Reid; Amie Steele; Christopher Turner; Erik Wilkins-McKee; Michael Willems; and Gregory Wilshusen made key contributions to this report.

Related GAO Products

High-Risk Series: An Update. [GAO-15-290](#). Washington, D.C: February 11, 2015.

Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems. [GAO-15-6](#). Washington, D.C: December 12, 2014.

Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts. [GAO-14-507](#). Washington, D.C.: September 15, 2014.

Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. [GAO-14-459](#). Washington, D.C.: June 5, 2014.

Climate Change Adaptation: DOD Can Improve Infrastructure Planning and Processes to Better Account for Potential Impacts. [GAO-14-446](#). Washington, D.C.: May 30, 2014.

Information Security: Agencies Need to Improve Cyber Incident Response Practices. [GAO-14-354](#). Washington, D.C.: April 30, 2014.

Climate Change: Energy Infrastructure Risks and Adaptation Efforts. [GAO-14-74](#). Washington, D.C.: January 31, 2014.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. [GAO-13-187](#). Washington, D.C.: February 14, 2013.

Critical Infrastructure Protection: DHS Could Better Manage Security Surveys and Vulnerability Assessments. [GAO-12-378](#). Washington, D.C.: May 31, 2012.

Cybersecurity: Threats Impacting the Nation. [GAO-12-666T](#). April 24, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. [GAO-12-92](#). Washington, D.C.: December 9, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. [GAO-11-865T](#). Washington, D.C.: July 26, 2011.

Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. [GAO-11-117](#). Washington, D.C.: January 12, 2011.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. [GAO-10-628](#). Washington, D.C.: July 15, 2010.

Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets. [GAO-10-147](#). Washington, D.C.: October 23, 2009.

Information Security: TVA Needs to Address Weaknesses in Control Systems Networks. [GAO-08-526](#). Washington, D.C.: May 21, 2008.

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

