



September 2018

DEFENSE INFRASTRUCTURE

Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts

Accessible Version

GAO Highlights

Highlights of [GAO-18-558](#), a report to the Committees on Armed Services, United States Senate and House of Representatives

Why GAO Did This Study

Since Congress provided statutory authority in 1997 for the privatization of utility systems at military installations, the military departments have privatized nearly 600 utility systems. According to DOD officials, utilities privatization enables military installations to obtain safe, reliable, and technologically current utility systems at a relatively lower cost than they would under continued government ownership.

The Senate report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 included a provision that GAO review DOD's utilities privatization program. This report assesses the extent to which DOD has (1) tracked utilities privatization contract performance and developed measurable performance standards, and (2) implemented cybersecurity guidance for industrial control systems associated with privatized utility systems. GAO reviewed relevant policies and internal control standards, analyzed a non-generalizable sample of utilities privatization contract documents, and interviewed DOD and selected military installation officials and privatized utility system owners.

What GAO Recommends

GAO recommends that DOD issue guidance requiring the military departments and DLA to develop metrics to track utilities privatization contract performance, and issue procedures concerning how the military departments are to determine what constitutes covered defense information as it relates to utilities privatization contracts. DOD concurred with both recommendations.

View [GAO-18-558](#). For more information, contact Brian J. Lepore at 202-512-4523 or leporeb@gao.gov

September 2018

DEFENSE INFRASTRUCTURE

Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts

What GAO Found

The military departments have some types of information about privatized utility systems, but they have not tracked contract performance or developed measurable performance standards for these contracts. Specifically:

- *Costs for Utility Infrastructure Improvements:* The military departments estimated the cost avoidance at the time of contract award; however, none of the military departments have determined whether the utilities privatization contracts are on track to achieve those estimates.
- *Costs for Utility Commodities:* Military department officials stated that they have observed reduced usage of commodity utilities, such as water usage, and thus decreased commodity costs, through utilities privatization; however, the officials have not tracked the data and any associated savings. Furthermore, the officials have not determined whether any savings were fully attributable to utilities privatization, recognizing that other factors may have affected commodity usage.
- *System Reliability:* Military department officials stated that they have perceived improvements in utility system reliability since utilities privatization and have access to contractor-provided data to assess reliability; however, the military departments have not used this data to determine reliability trends over time.
- *Contractor Performance Evaluations:* The military departments use the Contractor Performance Assessment Reporting System to evaluate each utility system owner's performance; however, based on GAO's review of the evaluations associated with the contracts in its sample, the evaluations were anecdotal and varied in frequency and quality.

Department of Defense (DOD) guidance does not require the development of metrics and associated measurable performance standards to track utilities privatization contract performance. Without a requirement to develop these metrics and standards, DOD will lack information on the performance of utilities privatization contracts and thus may not be able to perform effective program management and oversight for these long-term contracts.

DOD has taken steps to add a cybersecurity clause to its utilities privatization contracts that requires contractors take steps to ensure safeguards are put in place to protect covered defense information, which is defined as information that is processed, stored, or transmitted on the contractor's information system or industrial control systems. To implement the clause, DOD first must identify what, if any, covered defense information is provided to or developed by the contractor in performance of the contract. However, the Defense Logistics Agency (DLA) and military department officials stated that they have not begun to implement the clause because they need DOD to issue procedures concerning how the military departments are to determine what, if any, covered defense information associated with utilities privatization contracts is provided or developed by the contractor in performance of the contract. Without these procedures, the military departments and DLA will not have assurance that such information is being safeguarded.

Contents

Letter	1
Background	6
Military Departments Have Some Types of Information on Their Privatized Utility Systems, but Have Not Tracked Contract Performance or Developed Measurable Performance Standards	13
DOD Has Cybersecurity Requirements for Industrial Control Systems, but Has Not Begun to Implement Those Requirements for Utilities Privatization Contracts	20
Conclusions	28
Recommendations for Executive Action	30
Agency Comments and Our Evaluation	30
Appendix I: Selected Characteristics of the Department of Defense's (DOD) Utilities Privatization Contracts Included in GAO's Review	33
Appendix II: Comments from the Department of Defense	34
Appendix III: GAO Contact and Staff Acknowledgments	36
GAO Contact	36
Staff Acknowledgments	36
Appendix IV: Accessible Data	37
Agency Comment Letter	37
Related GAO Products	39
Tables	
Table 1: Status of Department of Defense Utilities Privatization, as of January 1, 2017	10
Table 2: Selected Characteristics of the Nine Utilities Privatization Contracts Included in Our Review	33

Figures

Figure 1: Example of a Potential Cyberattack Using False Data in an Industrial Control System	11
Figure 2: Responsibilities for Identifying, Marking, and Securing Covered Defense Information in Department of Defense (DOD) Contracts ^a	22

Abbreviations

ASD (EI&E)	Assistant Secretary of Defense for Energy, Installations and Environment
DLA	Defense Logistics Agency
DOD	Department of Defense
ICS	Industrial control systems

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.



September 4, 2018

Congressional Committees

Since Congress provided statutory authority in 1997 for the privatization of utility systems at military installations, the Department of Defense (DOD) has privatized nearly 600 of about 2,600 utility systems on military installations worldwide, including electric, water, wastewater, natural gas, and thermal systems.¹ According to the Office of the Assistant Secretary of Defense for Energy, Installations, and Environment (ASD (EI&E)), utilities privatization enables military installations to obtain safe, reliable, technologically current, and environmentally sound utility systems at a relatively lower cost than they would under continued government ownership. Utilities privatization gets DOD out of the business of owning, managing, and operating utility systems so that it can focus on its core missions and benefit from reliable utility systems owned and operated at industry standards.

DOD installations rely on the use of utilities, such as electricity and water, to accomplish their missions. Thus, DOD must be prepared for and adapt to changing conditions and withstand and recover rapidly from disruptions. This includes disruptions caused by deliberate attacks, such as cyberattacks on industrial control systems (ICS), accidents, and equipment failure, or naturally occurring events, such as severe weather.² According to DOD officials, such threats are a risk to ensuring the reliable provision of utility services to its installations. DOD has issued policies to its installations, including those with privatized utilities, to enhance energy

¹National Defense Authorization Act for Fiscal Year 1998, Pub. L. No. 105-85, § 2812 (Nov. 18, 1997), *codified as amended at* 10 U.S.C. § 2688. In December 1997, DOD issued Defense Reform Initiative Directive Number 9, which made utility system privatization a DOD policy. A year later, in December 1998, DOD issued another directive to establish program management and oversight responsibilities for the utilities privatization program, among other things. See, Deputy Secretary of Defense Memorandum, *Department of Defense Reform Initiative Directive #9—Privatizing Utility Systems* (Dec. 10, 1997), and Deputy Secretary of Defense Memorandum, *Department of Defense Reform Initiative Directive #49—Privatizing Utility Systems* (Dec. 23, 1998).

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 often found in the industrial sectors and critical infrastructure, including utility systems.

resilience, which the department defines as the ability to recover from energy disruptions that impact mission assurance on its installations. Various efforts can contribute to an installation's ability to achieve utility resilience, including upgrading and replacing utility infrastructure or equipment, which could be achieved through utilities privatization.

In our prior work since 2005, we identified multiple challenges with DOD's utilities privatization efforts and utilities resilience. In 2005, we identified several management weaknesses in DOD's implementation of the utilities privatization program.³ We made eight recommendations to help ensure the reliability of economic analyses and improve the utilities privatization guidance and procedures. DOD non-concurred with seven recommendations and partially concurred with one recommendation in its response to the report; however, DOD has since implemented all but one recommendation.⁴ In 2006, we reported that DOD's progress in implementing the utilities privatization program had been slower than expected and management concerns remained.⁵ We made seven recommendations to improve DOD's management of utilities privatization, and DOD generally concurred with and implemented six recommendations.⁶ In 2015, we identified that DOD faces challenges in implementing utility resilience efforts, such as collecting and reporting

³GAO, *Defense Infrastructure: Management Issues Requiring Attention in Utility Privatization*, [GAO-05-433](#) (Washington, D.C.: May 12, 2005).

⁴DOD partially concurred with our recommendation to revise its guidance for preparing economic analyses so that the analyses compare the cost of a proposed privatization contract with the cost of continued government ownership on the basis of the actual planned expenditures and the timing of these expenditures. DOD stated that it would continue to (1) use the appropriate industry standard in determining the long-term costs to the United States for utility services, and (2) develop tools for better predicting the requirements for providing adequate utilities services. However, DOD did not change its method for preparing the economic analyses and thus, considered this recommendation closed.

⁵GAO, *Defense Infrastructure: Actions Taken to Improve the Management of Utility Privatization, but Some Concerns Remain*, [GAO-06-914](#) (Washington, D.C.: Sept. 5, 2006).

⁶DOD disagreed with our recommendation to require each project's economic analysis to include the system's current annual costs and the actual expected annual costs if the system is not privatized. DOD stated that full implementation of its November 2005 guidance would provide further reassurance that every conveyance would reduce the long-term costs compared to the costs of continued ownership. However, as noted in our 2005 and 2006 reports, we believe that in the short term the utilities privatization program increases annual costs to the government where contractors make system improvements and recoup their costs from the department through their service contracts. We closed this recommendation in 2008 as not implemented.

comprehensive utility disruption data, and developing cybersecurity policies for its ICS.⁷ We made four recommendations to clarify utility disruption reporting guidance, improve data validation steps, and address challenges to addressing cybersecurity ICS guidance, and DOD concurred or partially concurred with all but one recommendation and implemented three recommendations.⁸

The Senate Armed Services Committee report accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 included a provision that we review DOD's utilities privatization efforts.⁹ In this report, we examined the extent to which the department has (1) tracked utilities privatization contract performance and developed measureable performance standards, and (2) implemented cybersecurity guidance for ICS associated with privatized utility systems.

For both objectives, we selected a non-generalizable sample of 9 utilities privatization contracts, which privatized 11 utility systems, as case studies to review.¹⁰ To select the case studies, we analyzed data maintained by ASD (EI&E) and the military departments to identify the universe of utility systems that were privatized using the legislative authority first granted by Congress in 1997. We determined that the data were sufficiently reliable for our objectives by comparing ASD (EI&E) data with the military department's data and interviewing military department officials about the data sources. Using this data, we selected contracts that had been awarded in 2007 or later, since we had previously reviewed the department's privatization efforts in 2005 and 2006.¹¹ From this group of contracts, we then selected at least three utility systems from each military department and at least one utility system of each type that was

⁷GAO, *Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning*, [GAO-15-749](#) (Washington, D.C.: July 23, 2015).

⁸DOD stated that it did not concur with our recommendation to revise the data collection template's instructions to include reporting of disruptions caused by DOD-owned infrastructure. The National Defense Authorization Act for fiscal year 2015 included an amendment that clarified the reporting requirement for DOD's Annual Energy Management Report and added a reporting requirement to include non-commercial utility outages involving DOD-owned infrastructure. As a result of congressional action, the intent of the recommendation has been met.

⁹S. Rep. No. 115-125 (2017).

¹⁰Two of the nine contracts privatized two utility systems. See appendix I for more information on the nine contracts.

¹¹See [GAO-05-433](#) and [GAO-06-914](#).

privatized—electric, water, wastewater, and natural gas in order to try and broadly capture the range of contracts.¹² For each of these contracts, we gathered detailed information from installation officials and representatives of the privatized utility system owner. In addition, we interviewed officials in ASD (EI&E) and the military departments' utilities privatization program management offices. Since our methodology was based on reviewing a select number of utilities privatization contracts in depth, we are unable to generalize the results from our review to the universe of DOD's utilities privatization contracts. Instead, this report highlights examples collected from the case studies identified above. Further information on the selected characteristics of the nine utilities privatization contracts included in our review can be found in appendix I.

For objective one, we reviewed DOD guidance on installation energy management and documentation from each military department on the performance of utilities privatization contracts.¹³ We also reviewed documentation describing any metrics and processes the military departments use to measure the performance of privatized utilities, including assessments of utility system owner performance. For each utility system and associated contract included in our sample, we reviewed the original contract and any subsequent modifications to the contract, as well as the associated documentation describing the metrics and processes used to measure progress and assess performance for each contract. We examined the modifications for each contract to calculate the changes in contract value over time. In presenting changes in contract value, we used constant dollars using a Gross Domestic Product deflator based on the year the contract was initially awarded.¹⁴ We also interviewed military department officials and utility system owners associated with each privatized utility system in our sample on performance metrics and on any challenges they experience in assessing the performance of privatized utilities. Because our scope was limited to utilities privatization contracts, we did not attempt to compare whether the reported performance results of utilities privatization might have been achieved through an alternative approach, such as continued government

¹²The Department of the Navy manages the utilities privatization contracts for the U.S. Marine Corps.

¹³DOD Instruction 4170.11, *Installation Energy Management* (Dec. 11, 2009) (incorporating Change 1, effective Mar. 16, 2016).

¹⁴The Gross Domestic Product deflator is a measure of price inflation. We used this measure to compare current contract values with the contract values at the time of award so that we could determine the price increase in real terms.

ownership or other alternative financing arrangements such as energy savings performance contracts.¹⁵ We compared ASD (EI&E) and military department efforts to monitor utilities privatization performance with Standards for Internal Control in the Federal Government and our prior work on strategic planning to determine whether ASD (EI&E) or the military departments have implemented controls, such as the establishment of performance metrics, which may be necessary to achieve department objectives efficiently and to gauge progress toward meeting department objectives.¹⁶

For objective two, we reviewed DOD guidance and documentation to identify and describe policies regarding requirements for cybersecurity of ICS associated with privatized utility systems, including requirements in the Defense Federal Acquisition Regulation Supplement.¹⁷ We interviewed officials from ASD (EI&E) and the military departments' utilities privatization program management offices about policies regarding requirements for cybersecurity of ICS and the implementation of these policies. In addition, we examined the utilities privatization contracts included in our sample to identify and describe the extent to which the contracts characterize any requirements for cybersecurity. We interviewed military department officials, Defense Logistics Agency (DLA) officials, and contractors associated with each privatized utility system included in our sample to determine how these officials have implemented cybersecurity for ICS associated with privatized utility systems. We also compared the department's utilities privatization policies on cybersecurity with Standards for Internal Control in the Federal Government requirements for management to evaluate security threats to information technology, including ICS, which can come from both internal and external sources, and periodically review policies and

¹⁵DOD uses alternative financing arrangements in addition to using up-front appropriations to fund a portion of its infrastructure related to renewable energy generation, energy efficiency, power generation, and energy security on military installations. These alternative financing arrangements include energy savings performance contracts, utility energy service contracts, power purchase agreements, and some forms of enhanced use leases.

¹⁶GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014).

¹⁷Department of Defense, Defense Federal Acquisition Regulation Supplement clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct. 21, 2016).

procedures for continued relevance and effectiveness in addressing related risks facing the entity as it seeks to achieve its objectives.¹⁸

We conducted this performance audit from July 2017 to September 2018 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

Utilities Privatization Authorities and Intent

Congress provided statutory authority in 1997 for the privatization of utility systems on military installations to address DOD's need to supply reliable, safe, and efficient utility services to its installations.¹⁹ In defining a utility system, the authority includes systems for the generation and supply of electric power; the treatment or supply of water; the collection or treatment of wastewater; the generation or supply of steam, hot water, and chilled water; the supply of natural gas; and the transmission of telecommunications.²⁰ Included in a utility system are the associated equipment, fixtures, structures, and other improvements, as well as real property, easements, and rights-of-way. The authority states that the Secretary of a military department may convey a utility system to a municipal, private, regional, district, or cooperative utility company or other entity. DOD's policy permits the military departments to maintain ownership of utility systems and not privatize them for unique security

¹⁸[GAO-14-704G](#).

¹⁹National Defense Authorization Act for Fiscal Year 1998, Pub. L. No. 105-85, § 2812 (Nov. 18, 1997), codified as amended at 10 U.S.C. § 2688. Congress has amended the legislation 10 times since 1998.

²⁰Section 2813 of the National Defense Authorization Act for Fiscal Year 2017 states: "It is the sense of Congress that the reference to a system for the collection or treatment of wastewater in the definition of 'utility system' in section 2688 of title 10, United States Code, which authorizes the Department of Defense to convey utility systems, includes stormwater systems and components." Pub. L. No. 114-328, § 2813 (Dec. 23, 2016). However, this report does not discuss privatized stormwater systems because the department has not privatized any stormwater systems.

reasons, such as installations with highly sensitive missions, or when privatization is uneconomical.²¹

Utilities Privatization Roles and Responsibilities

ASD (EI&E) oversees DOD's utilities privatization program, which is part of the department's installation energy management portfolio. In this capacity, ASD (EI&E) is responsible for developing policies and overseeing the program. There are two main sources of guidance for utilities privatization— a DOD instruction on energy management at the installation level, DOD Instruction 4170.11, *Installation Energy Management*, and a series of memorandums specific to utilities privatization.²² The instruction and memorandums direct the military departments to attempt to privatize all utility systems, unless the Secretary of the military department determines that the system is exempt from privatization for security or economic reasons. Some of the memorandums were issued to provide the military departments with guidance to implement certain changes to the statutory authority related to utilities privatization. For example, the congressional authority was amended in 2006 to require the Secretary of Defense's (or a designee's) approval for utilities privatization contracts with terms longer than 10 years, but not to exceed 50 years.²³ The subsequent guidance memo delegated the approval from the Secretary of Defense to the Secretaries of the military departments and the Director of the DLA.²⁴

²¹A system may be deemed uneconomical to privatize only when there is a demonstrated lack of market interest or when the costs to the government exceed the benefits. A system might be exempted from privatization for security reasons in situations where non-federal ownership would create an unacceptable risk to a military department's mission or compromise classified operations or property. See DOD Instruction 4170.11, *Installation Energy Management* (Mar. 16, 2016).

²²DOD Instruction 4170.11, *Installation Energy Management* (Dec. 11, 2009) (incorporating Change 1, effective Mar. 16, 2016). As stated earlier, in 1997 and 1998, the Deputy Secretary of Defense issued two directives on utilities privatization. The 1998 guidance established program management and oversight responsibilities and provided guidance for performing economic analyses for proposed utilities privatization projects, exempting systems from the program, and using competitive procedures to conduct the program. Subsequently, in 2002, the department revised its utilities privatization guidance, which replaced the guidance issued in 1998.

²³National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163 §2823 (Jan. 6, 2006), *codified as amended* at 10 U.S.C. § 2688(d).

²⁴Office of the Under Secretary of Defense for Acquisition, Technology and Logistics Memorandum, *Supplemental Guidance for the Utilities Privatization Program* (Mar. 20, 2006).

The military departments have the responsibility for program implementation, as the statutory authority to privatize utility systems is granted to the Secretaries of the military departments. As such, the military departments determine which systems will be privatized and which systems may be exempted from privatization due to economic or security reasons. According to military department officials, each military department considers utilities privatization as an option for the recapitalization of utility infrastructure.²⁵ The Army views utilities privatization as the preferred option, while the Navy and the Air Force consider utilities privatization to be one option among others. Specifically,

- Army officials stated that they follow the statute and ASD EI&E program guidance documents. Those documents state that utilities privatization is the preferred method for recapitalizing utility infrastructure and officials stated that the Army plans to assess all of its utility systems for privatization. The Army prioritizes systems in the worst condition and systems with important missions for privatization.²⁶ According to Army officials, in cases where the utility system is in poor condition and the installation performs important missions, the Army may privatize utility systems even if the costs in the contractor's proposal exceed the costs in the government's "should cost" estimate by as much as 15 percent.²⁷
- The Air Force's utilities privatization policy states that the program's goal is to permanently convey utility systems on Air Force active, reserve, and guard installations to private or public utility companies in conjunction with an award of a long-term utility services contract for the operation and maintenance of those systems.²⁸ The purpose of privatizing a utility system is to restore utility infrastructure to industry standards for operations,

²⁵According to DOD, recapitalization includes the restoration, modernization, or replacement of facilities or their structural components to extend or restore a facility's lifecycle.

²⁶Department of the Army, Office of the Assistant Chief of Staff for Installation Management, *Utilities Privatization (UP) Schedule and FY 15 Strategic Priorities* (July 28, 2014).

²⁷The government's "should cost" estimate is an estimate of the costs of continued government ownership assuming that the military service would upgrade, operate and maintain the system in accordance with accepted industry standards as called for in the proposed privatization contract.

²⁸Department of the Air Force, *Providing Utilities to U.S. Air Force Installations*, 32-1061 (Jun. 2018).

maintenance, recapitalization, health, and safety while achieving a monetary savings over the cost of continued Air Force ownership.

- According to Navy officials, the Navy has not pursued utilities privatization in recent years but is currently in the process of assessing utility systems for potential conveyance. Any decisions to convey utility systems will be based on a business case analysis for total ownership cost and the ability to improve reliability, resilience, and efficiency for priority missions. Navy officials noted that the Navy follows DOD policy for utility conveyance authority.

DLA works with the military departments to plan for utilities privatization and procures and administers 61 utilities privatization contracts for the Departments of the Army and Air Force from the pre-solicitation phase and into the post-award phase. According to DLA officials, the entire pre-award process takes approximately 915 days, based on the assumption that the solicitation receives 1 to 6 proposals from contractors. Once an award decision is made, privatization involves two transactions with the successful contractor—the conveyance of the utility system infrastructure and the acquisition of utility services for upgrades, operations, and maintenance under a long-term contract of up to 50 years. According to DLA officials, the contract term can be up to 50 years because it allows the military departments the opportunity to spread the high costs to repair and replace existing utility infrastructure over a long period of time. The Department of the Navy administers its own utilities privatization contracts for Navy and Marine Corps installations.

DOD's Privatization of Utility Systems Since 1988

As of January 2017, the military departments have privatized approximately 23 percent (601 of 2,574) of their utility systems.²⁹ As shown in table 1, the Army has privatized the most systems (369), followed by the Air Force (174), and then the Navy (58). In addition, table 1 shows the number of utility systems the military departments have exempted for either economic or security reasons. As of January 2017,

²⁹According to an ASD EI&E official, data as of January 2017 was the most current data available. Before and after approval of the specific authority for privatizing utilities the services have used other authorities for utilities privatization. For example, the Army had privatized some systems after obtaining congressional authority for each specific case. Also, the services have privatized systems by modifications to natural gas services agreements administered by the General Services Administration and by conveyances of some systems on the basis of authorities related to base realignment and closure and the military housing privatization program.

the military departments have 600 systems that have not been privatized or exempted from privatization. The Army and the Air Force have plans to privatize more systems in the coming years.

Table 1: Status of Department of Defense Utilities Privatization, as of January 1, 2017

Military department	Privatized utility systems	Utility systems exempted from privatization ^a	Utility systems owned by others ^b	Active utility systems ^c	Total utility systems
Army	369	6	489	236	1,100
Air Force	174	163	59	264	660
Navy	58	489	167	100	814
Total	601	658	715	600	2,574

Source: Department of Defense. | GAO-18-558

^aUtility systems may be exempted from privatization for economic or security reasons.

^bUtility systems owned by others include systems that were built and are maintained by an entity other than the United States government.

^cActive utility systems includes all utility systems that have not been privatized or exempted from privatization.

Industrial Control System Vulnerabilities and Cybersecurity Policies and Guidance

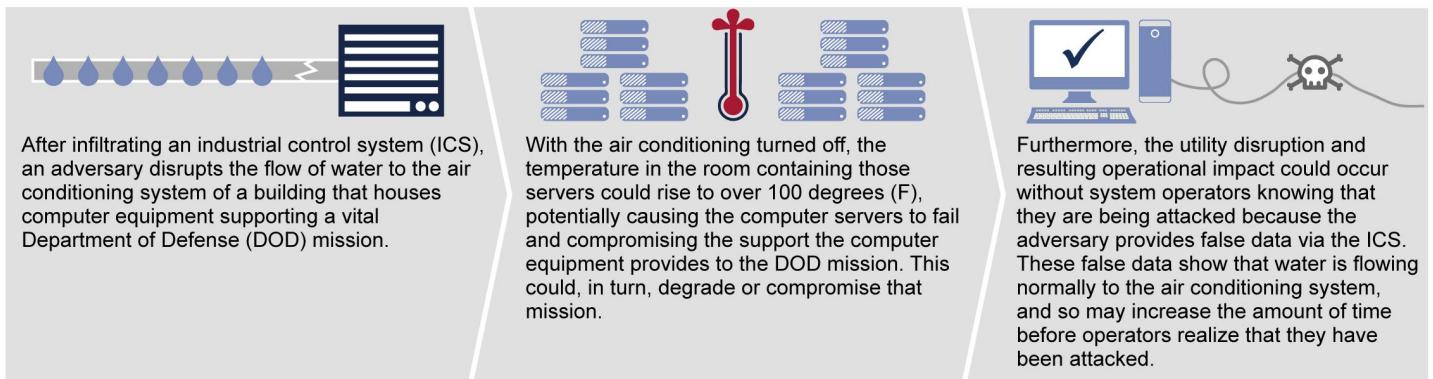
According to an ASD (EI&E) official, information residing on ICS associated with privatized utilities systems, and more broadly, information on any ICS, may be used by adversaries to gain insights into operations on installations or to conduct a cyberattack.³⁰ According to U.S. Cyber Command, DOD’s ICS are a potential target and an adversary could gain unauthorized access and attack DOD in a variety of ways, including removing data from an ICS, inserting false data to corrupt the monitoring and control of utility infrastructure through ICS, and physically destroying utility infrastructure controlled by an ICS.³¹ As such, DOD’s 2015 Cyber Strategy recognizes the need to protect DOD information regardless of where it resides—on DOD’s own information systems and ICS or on

³⁰ICS, regardless of ownership, may be vulnerable to cyberattacks, as noted in the National Institute of Standards and Technology guide to ICS cybersecurity. The guide notes that ICS are critical to the operation of the U.S. critical infrastructures and that approximately 85 percent of these infrastructures are privately owned and operated. Federal agencies also operate many similar industrial processes as well as air traffic control. See National Institute of Standards and Technology, Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, Revision 2 (May 2015).

³¹[GAO-15-749](#).

contractor-owned information systems and ICS— so that DOD capabilities are not exploited, misdirected, countered, or cloned. Figure 1 illustrates a potential cyberattack using false data in an ICS.

Figure 1: Example of a Potential Cyberattack Using False Data in an Industrial Control System



Source: GAO analysis of DOD information. | GAO-18-558

In addition, there have been reports of successful attacks using ICS associated with infrastructure. Specifically, the Office of the Director of National Intelligence issued a report in 2017 describing several of these attacks.³² For example, the report noted that in 2010, Stuxnet was the first computer virus specifically targeting ICS, and it allowed attackers to take control of the systems and manipulate real-world equipment without the operators knowing. The attacker targeted certain equipment at the Natanz uranium enrichment plant in Iran, manipulated computer systems that control and monitor the speed of the centrifuges, and reportedly destroyed roughly one-fifth of Iran’s nuclear centrifuges by causing them to spin out of control. The attacker increased the pressure on spinning centrifuges while showing the control room that everything appeared normal by replaying recordings of the plant’s protection system values during the attack. In another example, the report noted that in 2012, a U.S. power utility’s ICS was infected with a virus when a third-party technician used an infected USB drive to upload software to the systems. The virus resulted in downtime for the systems and delayed plant restart by approximately 3 weeks.

³²The Public-Private Analytic Exchange Program, *Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions* (2017). The report’s objective was to recommend risk mitigation strategies and measures and to highlight potential security risks to ICS.

In recognition of these threats, DOD has developed cybersecurity policies and guidance for ICS that apply to both DOD-owned ICS and contractor-owned ICS.³³ Specifically,

- For DOD-owned ICS, the department has issued several policies and guidance for the cybersecurity of ICS. For example, in 2016, in response to one of our prior recommendations that ASD (EI&E) address challenges the military services faced in implementing the risk management framework guidance, ASD (EI&E) directed the services to develop plans identifying the goals, milestones, and resources needed to identify, register and implement cybersecurity controls on DOD facility-related ICS.³⁴ Further, DOD issued additional guidance that was intended to assist the military services in developing implementation plans to meet these requirements. In 2016, DOD issued guidance, in the form of Unified Facilities Criteria, which provides criteria for the inclusion of cybersecurity in the design of control systems in order to address appropriate security controls during design and subsequent construction.³⁵ Also, in 2016, the U.S. Cyber Command and the Office of the Secretary of Defense issued guidance that identifies device anomalies that could indicate a cyber incident, specific detection procedures to assess the anomaly, and

³³GAO has reported on other topics related to DOD's implementation of cybersecurity strategies. For example, see GAO, *Defense Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened*, [GAO-17-512](#) (Washington, D.C., Aug. 1, 2017), and GAO, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, [GAO-17-668](#) (Washington, D.C., July 27, 2017). Other federal agencies, such as the Department of Energy, the Department of Homeland Security, and the Federal Energy Regulatory Commission have responsibilities related to the resilience of the electric grid. The Federal Energy Regulatory Commission, which regulates the interstate transmission of electricity, is responsible for reviewing and approving standards developed by the North American Electric Reliability Corporation to provide for the reliable operation of the bulk power system. These standards include requirements for planning and operating the bulk power system to provide for its reliable operation, including standards for cyber security. For example, in April 2018, the Federal Energy Regulatory Commission approved a standard clarifying obligations pertaining to electronic access controls for certain cyber systems, among other things.

³⁴DOD's risk management framework guidance is included in DOD Instruction 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT) (Mar. 12, 2014)(incorporating Change 2, effective July 28, 2017). See [GAO-15-749](#).

³⁵DOD, Unified Facilities Criteria (UFC) 4-010-06: Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems (Sept. 19, 2016).

procedures to recover electronic devices, including removing and replacing the device.³⁶

- For contractor-owned ICS, including ICS owned by privatized utility system owners, DOD has a Defense Federal Acquisition Regulation Supplement clause to require that contractors take steps to ensure safeguards are put in place to protect covered defense information, which is defined as unclassified controlled technical information or other information that is processed, stored, or transmitted on the contractor's information system or ICS.³⁷ Controlled unclassified information is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies. The clause also requires the contractor to report cyber incidents.

Military Departments Have Some Types of Information on Their Privatized Utility Systems, but Have Not Tracked Contract Performance or Developed Measurable Performance Standards

The military departments have information about utility systems that have been privatized, but they have not tracked utilities privatization contract performance or developed measurable performance standards for these contracts. Specifically, for the systems in our sample the military departments have some information on the costs for utility infrastructure improvements and commodities, system reliability, and contractor performance evaluations.

³⁶U.S. Cyber Command and Office of the Secretary of Defense, Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS), version 1.0 (January 2016).

³⁷Department of Defense, Defense Federal Acquisition Regulation Supplement clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct. 21, 2016). According to DOD, adequate security for covered defense information requires, at a minimum, the implementation of National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations. This special publication is a set of standards that define how owners of non-federal information systems can safeguard and distribute information deemed sensitive but not classified. DOD considers the definition of covered defense information to be in line with the definition for controlled unclassified information, which is information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls.

- *Costs for Utility Infrastructure Improvements:* The military departments have information on the estimated cost avoidance at the time of contract award for utility infrastructure improvements; however, none of the military departments have determined whether the utilities privatization contracts are on track to achieve those cost avoidance estimates. For example, officials at Fort Bragg, North Carolina, estimated at the time of contract award that it would have cost the Army \$61.4 million to provide natural gas utility services over the life of the utilities privatization contract, while the successful proposal from the contractor estimated a cost of \$52.3 million for the same services. Therefore, the Army initially projected that it would avoid an estimated cost of \$9.1 million for natural gas utility services at Fort Bragg over the life of the contract.

However, the estimate at the time of contract award used by each military department does not account for changes in the cost of the contract over time. Moreover, none of the military departments measure actual cost avoidance over time, and some utilities privatization contracts have experienced cost increases. Specifically, we found that six of the nine utilities privatization contracts in our sample included modifications, which increased the original cost of the contract by more than 5 percent after adjusting for inflation.³⁸ For example, the contract to privatize electric and water services at Tyndall Air Force Base, Florida, had 59 modifications, which have increased the total estimated contract value by 36 percent (\$42 million) to \$159 million since it was awarded in September 2010.³⁹ In addition, the water and wastewater privatization contract at Fort Bragg had 219 modifications, which has increased the total estimated

³⁸According to installation officials, modifications to the utilities privatization contract may occur if the installation decides to privatize additional infrastructure or more extensive repairs are needed than originally estimated. According to our analysis of the contract modifications associated with the Navy contracts in our non-generalizable sample, the electric utilities privatization contract at Naval Air Station Corpus Christi, Texas, and the wastewater utilities privatization contract at Naval Air Station Key West, Florida, did not experience net cost growth in contract value from award to April 2018.

³⁹For our analysis for Tyndall Air Force Base, we adjusted for inflation the 2018 total contract value to constant 2010 dollars using a Gross Domestic Product index to calculate the 34 percent change. The Gross Domestic Product index is a measure of price inflation. We used this measure to compare current contract values with the contract values at the time of award so that we could determine the price increase in real terms. The April 2018 Tyndall Air Force Base total contract value documented on the latest contract amendment was \$179 million, an increase of \$61 million in nominal terms from the original contract cost.

contract value by 96 percent (\$552 million) to about \$1.1 billion since it was awarded in September 2007.⁴⁰

According to military department and DLA officials, there are limitations to using the information in the modifications to analyze changes in cost over time associated with the utilities privatization contracts because some cost changes may have occurred even if the government had retained ownership of the utility system. DLA officials stated that the modifications are made for a number of different reasons, including changes in mission requirements, changes to the utility service requirements, and capital upgrade projects on the installation. According to military department officials, cost changes associated with changes in the installation's mission would likely have occurred had the military department retained ownership and would not be a cost increase due to privatization. Thus, it is difficult to determine the extent to which cost increases affect the cost avoidance estimated at the time of contract award.

In 2006, we reported that cost growth in DOD's utilities privatization contracts may become a concern because once a utility system is privatized, the government enters into a sole-source relationship with the privatized utilities system owner, which may put the government at a disadvantage when negotiating prices for utility system changes.⁴¹ To mitigate this disadvantage, DLA and Air Force officials stated that they use experts who review proposals from the privatized utility system owners to help ensure that costs are fair and reasonable.

- *Costs for Utility Commodities:* Military department officials stated that they have observed reduced usage of the commodity provided by the utility, such as water usage, and thus decreased commodity costs through utilities privatization; however, installation officials have not tracked the data and associated savings. Furthermore, the officials have not determined whether any savings were fully attributable to utilities privatization, recognizing that other factors may have affected commodity usage. For example, officials at Tyndall Air Force Base,

⁴⁰For our analysis for Fort Bragg, we adjusted for inflation the 2018 total contract value to constant 2007 dollars using a Gross Domestic Product index to calculate the 96 percent change. The Gross Domestic Product index is a measure of price inflation. We used this measure to compare current contract values with the contract values at the time of award so that we could determine the price increase in real terms. The April 2018 Fort Bragg total contract value documented on the latest contract amendment was \$1.3 billion, an increase of \$763 million in nominal terms from the original contract cost.

⁴¹[GAO-06-914](#).

Florida, stated that repairs to their privatized water system infrastructure have resulted in less water usage, and that there has been a decrease in the number of leaks. An Army official estimated commodity cost savings by comparing commodity costs prior to utilities privatization with commodity costs after utilities privatization. This approach was based on the assumption that any such savings were primarily due to utilities privatization. However, an Army official stated that the commodity cost savings the Army estimated could be attributed to other factors outside of utilities privatization, such as decreases in base population or execution of Energy Savings Performance Contracts.⁴² Air Force and Navy officials stated they did not estimate commodity cost savings.

- *System Reliability*: Military department officials stated that they have perceived improvements in utility system reliability since utilities privatization and have access to contractor-provided data to assess reliability; however, the military departments have not used the contractor-provided data to determine reliability trends over time. For example, Army officials at Arlington National Cemetery, Virginia, stated that they could not recall an unscheduled outage since the privatization of the electric system in 2015. In addition, officials at Tyndall Air Force Base, Florida, stated that there was a significant drop in outages after the electric system was privatized in 2010. However, we found that none of the military departments have formally measured improvements in reliability due to utilities privatization, because, according to military installation officials, they did not track reliability statistics prior to utilities privatization nor were they required to do so. In addition, we found that not all installations in our sample of cases have analyzed contractor-provided outage data, which includes information on the number of scheduled and unscheduled outages and the causes of the outages, to verify perceived reliability improvements. However, officials at Hill Air Force Base, Utah, stated that the system owner provides reports that track reliability over time and trends could be determined through this data collection. As we previously reported, there are benefits to collecting utility disruption information since it can be used to identify repairs and to prioritize funding for those repairs.⁴³

⁴²Energy Savings Performance Contracts allow federal agencies to procure energy savings and facility improvements with no up-front capital costs or special appropriations from Congress. An Energy Savings Performance Contract is a partnership between an agency and an energy service company.

⁴³GAO, *Defense Infrastructure: Actions Needed to Strengthen Utility Resilience Planning*, [GAO-17-27](#) (Washington, D.C.: Nov. 14, 2016).

- **Contractor Performance Evaluations:** The military departments use the Contractor Performance Assessment Reporting System to subjectively evaluate each utility system owner's performance across several categories, including management, schedule, and cost control, among others; however, based on our review of the evaluations associated with the nine contracts in our sample, we found that the evaluations were anecdotal and varied in frequency and quality.⁴⁴ While we found that the assessing officials generally reported satisfactory system owner performance, the performance periods in the evaluations varied. For example, one evaluation for the water privatization contract at Naval Air Station Key West, Florida, covered 4 years, while the subsequent evaluation for the same contract covered 1 year. Another evaluation for the natural gas privatization contract at Fort Bragg, North Carolina, covered a performance period of 1 year and 4 months. Guidance for these contractor assessments indicates that agencies should conduct contractor performance evaluations on an interim annual basis and upon final completion of the contract.⁴⁵ In addition, evaluation information supporting ratings varied. In one evaluation for the electric and water privatization contract at Tyndall Air Force Base, Florida, an assessing official cited multiple concerns in the supporting narrative for an evaluation area and rated it as "unsatisfactory," while the

⁴⁴The Federal Acquisition Regulation requires that contractor performance information be collected and used in source selection evaluations. In general, assessment guidance indicates that clear and timely performance evaluations help agencies make informed decisions when awarding contracts and ensures that the government does business with companies that provide quality products and services in support of agencies' missions. Through the Contractor Performance Assessment Reporting System, the assessing official completes past performance evaluations, which rate the utility system owner on various elements such as quality of the product or service, schedule, cost control, management, and regulatory compliance. For each applicable rating element, the assessing official determines a rating based on definitions from the Contractor Performance Assessment Reporting System Guide that generally relates to how well the utility system owner met the contract requirements and responded to problems. In addition, for each rating element, a written narrative is used to provide support for the rating assigned.

⁴⁵Contractor Performance Assessment Reporting System Program Office, *Guidance for the Contractor Performance Assessment Reporting System (CPARS)*, (August 2017). The guidance provided in this document is based on the authorities prescribed by the Federal Acquisition Regulation and agency supplements. The guidance is non-regulatory in nature and intended to provide useful information to the workforce for using the Contractor Performance Assessment Reporting System. The guidance should be read in conjunction with the Federal Acquisition Regulation parts related to past performance information. Additional guidance may be provided by respective agency policies but should not conflict with the Federal Acquisition Regulations or the guide.

subsequent evaluation for the same contract provided an “exceptional” rating for the same evaluation area with no explanation of how previous concerns were addressed.

The military departments have not tracked utilities privatization contract performance and have not developed measurable performance standards because ASD (EI&E) has not issued guidance requiring the military departments to develop metrics and measurable performance standards. *Standards for Internal Control in the Federal Government* state that management should design control activities—such as the establishment of performance measures and indicators—to achieve objectives.⁴⁶ In addition, our prior work has shown that an element of sound planning focuses on developing a set of metrics that will be applied to gauge progress toward attainment of the plan’s long-term goals.⁴⁷ The metrics can be used to evaluate the plan through objective measurement and systematic analysis to determine the manner and extent to which privatized utility systems meet measurable performance standards. According to our prior work, performance measurement focuses on whether a program has achieved its objectives, expressed as measurable performance standards.⁴⁸ Moreover, DOD’s guidebook for the acquisition of services states that services acquisition is about acquiring performance results that meet performance requirements needed to successfully execute an organization’s mission. Those performance requirements and how the government will assess the contractor’s performance must be determined before the contract is awarded.⁴⁹

⁴⁶[GAO-14-704G](#).

⁴⁷GAO’s leading practices for sound planning are derived from prior work related to strategic planning. For example, *Defense Logistics: Actions Needed to Improve the Marine Corps’ Equipment Reset Strategies and the Reporting of Total Reset Costs*, [GAO-11-523](#) (Washington, D.C.: Aug. 4, 2011), and GAO, *Managing for Results: Critical Issues for Improving Federal Agencies’ Strategic Plans*, [GAO/GGD-97-180](#) (Washington, D.C.: Sept. 16, 1997). These leading practices are based on GAO’s past review of 27 agencies’ draft strategic plans. GAO used the Results Act supplemented by the Office of Management and Budget’s guidance on developing plans (Circular A-11, part 2) as criteria to determine whether draft plans complied with the requirement for six specific elements that are to be in strategic plans.

⁴⁸GAO, *Performance Measurement and Evaluation: Definitions and Relationships*, [GAO-11-646SP](#) (Washington, D.C.: May 2, 2011).

⁴⁹DOD, *Guidebook for the Acquisition of Services* (Mar. 24, 2012). According to the guidebook, the services acquisition process has three phases—planning, development, and execution—and each phase builds on the knowledge gained in the previous phase.

DOD has guidance that requires the military departments to conduct a post-conveyance review for each privatized utility system. That guidance states that the military departments shall compare utilities privatization costs after the contract award to projected costs to identify whether there is a problem with cost growth.⁵⁰ The guidance does not require the development of metrics and associated measurable performance standards to report on the performance of utilities privatization contracts.

ASD (EI&E) officials stated that performance metrics are needed to improve DOD's oversight of utilities privatization efforts. According to *Standards for Internal Control in the Federal Government*, it is important for management to design performance metrics and standards because they help the entity achieve its goals. For example, ASD (EI&E) officials stated that they issued a data call to the military departments in January 2017 requesting information about the performance of utilities privatization contracts. Officials noted that they received different information from each military department and did not believe that the information would enable the department to determine whether the privatized utilities systems are improving reliability or achieving the cost savings originally estimated. For example, these officials stated that some installations provided contractor performance evaluation ratings, but these ratings were anecdotal and could not be used to determine improved reliability or estimated cost savings. Air Force officials also stated that they needed performance metrics to improve their management of utilities privatization. Officials explained that the information they receive from contracting officers and contracting officer representatives specific to privatized utilities is anecdotal and qualitative, and they have no metrics in place that allow the Air Force to track the performance of utilities privatization contracts over time or to identify trends and issues that would enable the Air Force to take steps to improve utilities privatization. However, Air Force officials stated that the Air Force is working on developing a standardized reporting template, called the Monthly System Performance Report, which will enable the Air

⁵⁰DOD Instruction 4170.11, *Installation Energy Management*, states that the military departments shall conduct a post-conveyance review of each privatized system 2 to 3 years after award or 1 year after the first price re-determination, whichever is later. This timeframe allows for proper contractor transition and steady state operation. A post-conveyance review shall include, at a minimum, joint detailed inventory, updated list of requirements reflecting changes, updated list of transition requirements, updated list of deficiencies, contract cost changes due to updated inventory, contract cost changes due to new connections or disconnects, and description of inventory changes due to connections and disconnects.

Force to track reliability for its privatized utility systems and to identify reliability trends over time.⁵¹

DOD's utilities privatization program has been in place for 21 years and some information, such as the contractor-provided reliability data, is available that could be used to track performance over time. Performance metrics and standards would help ASD (EI&E) track the outcomes of the utilities privatization program. In addition, the life of utilities privatization contracts can extend to 50 years, producing a long-term, one-to-one relationship between the utility system owner and the government. The ability of ASD (EI&E), DLA, and the military departments to track performance over the life of utilities privatization contracts may help mitigate the risks of being in a one-to-one relationship with the utility system owner. Without issuing guidance that requires the military departments and DLA to develop and implement metrics and measurable performance standards to track contract performance for future utilities privatization contracts and to develop similar guidance for current utilities privatization contracts, the department will lack information on the performance of utilities privatization contracts. As a result, ASD (EI&E), the military departments, and DLA may not be able to perform effective program management and oversight for these long-term utilities privatization contracts.

DOD Has Cybersecurity Requirements for Industrial Control Systems, but Has Not Begun to Implement Those Requirements for Utilities Privatization Contracts

DOD Has Cybersecurity Requirements for Industrial Control Systems

In November 2013, DOD issued guidance in the form of a Defense Federal Acquisition Regulation Supplement clause to establish minimum requirements for safeguarding covered defense information on a

⁵¹The Army headquarters official we met with did not identify performance metrics used by the Army to track the performance of privatized utility systems after contract award, but stated that the utility system owners had methods of tracking performance. The Navy headquarters officials we spoke with stated that the Navy is in the process of revitalizing its utilities privatization efforts to support the recapitalization of its utility infrastructure.

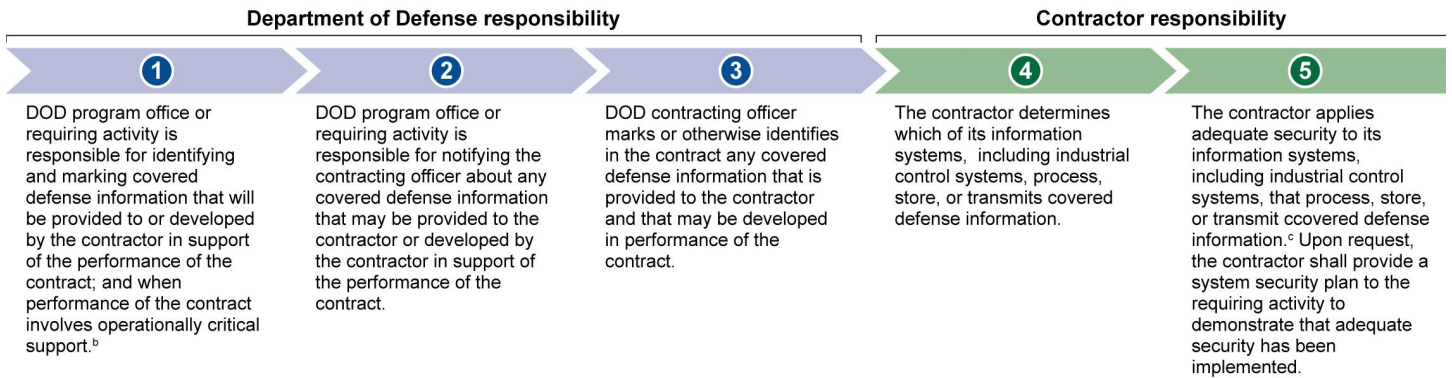
contractor's ICS.⁵² The clause requires contractors to implement a minimum set of security controls on contractor information technology and ICS, to report cyber incidents, and to support DOD damage assessments as needed.⁵³ According to DOD, the Defense Federal Acquisition Regulation Supplement clause for safeguarding covered defense information is required to be added to all new solicitations and contracts as of November 2013. The clause is not required to be incorporated retroactively into DOD contracts awarded prior to 2013, but that does not preclude a contracting officer from modifying existing contracts to incorporate the clause.

To implement the clause for safeguarding covered defense information, the contractor must apply a minimum set of security controls on its ICS. For the contractor to know what the appropriate security controls are, DOD first must identify what, if any, covered defense information is provided to or developed by the contractor in performance of the contract. If the requiring activity determines that covered defense information is provided to or developed by the contractor, then the contracting officer notifies the contractor by documenting what information is considered covered defense information. Then, to secure DOD's covered defense information, the contractor must apply adequate security to its ICS on which that information resides and document, in a system security plan, how the requirements were met or how the contractor plans to meet the requirements. When requested by the requiring activity, the system security plan should be submitted to demonstrate that adequate security has been implemented. Figure 2 shows the responsibilities for identifying, marking, and securing DOD's covered defense information on contractor information and industrial control systems.

⁵²Defense Federal Acquisition Regulation Supplement clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (Oct. 21, 2016). The clause applies to all types of information systems, to include business information general purpose information systems as well as ICS. However, since our research was focused on this clause as it relates to cybersecurity requirements for ICS associated with privatized utility systems, we refer specifically to ICS throughout the report.

⁵³The minimum set of security controls required are described in National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. This publication applies to information and industrial control systems. DOD guidance acknowledges that the industrial environments may require different controls than those used for business environments because industrial environments may require controls for the integrity of the data and the availability of the system. The special publication was structured such that the contractor's operations would dictate the selection of the appropriate controls for their internal system.

Figure 2: Responsibilities for Identifying, Marking, and Securing Covered Defense Information in Department of Defense (DOD) Contracts^a



Source: GAO analysis of Department of Defense (DOD) information. | GAO-18-558

Notes

^aCovered defense information is defined as unclassified controlled technical information or other information that is processed, stored, or transmitted on the contractor’s information system or ICS. Controlled unclassified information is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies. See Department of Defense, Defense Federal Acquisition Regulation Supplement clause 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct. 21, 2016).

^bGuidance on marking materials can be found in DOD Manual 5200.01, Volume 4, DOD Information Security Program: Controlled Unclassified Information (CUI)(Feb. 24, 2012)(incorporating Change 1, effective May 9, 2018).

^cAdequate security, according to DOD, requires, at a minimum, the implementation of National Institute of Standards and Technology Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (December 2016).

DOD Has Not Begun to Implement Cybersecurity Requirements for Utilities Privatization Contracts

DOD officials stated that while they have taken steps to incorporate the clause requiring the safeguarding of covered defense information into many of their utilities privatization contracts, they have not begun to implement the cybersecurity requirement in the clause to ensure that covered defense information is appropriately safeguarded for those contracts. DLA, Army, and Air Force officials stated that they have added cybersecurity requirements to some of the utilities privatization contracts they administer, but the Navy has not. Specifically:

- *DLA*: According to DLA officials, of the 61 privatized utility contracts DLA manages on behalf of the Army and Air Force, officials have incorporated the clause requiring the safeguarding of DOD covered

defense information into 60 contracts, and are in the process of modifying one contract to incorporate the clause.⁵⁴ According to DLA officials, beginning in June 2015, they determined that the utilities privatization contracts needed to be modified to incorporate the cybersecurity requirements to safeguard DOD covered defense information associated with its utilities privatization contracts for two reasons.⁵⁵ First, DLA officials stated that they interpreted DLA-contracting guidance issued in 2015 to direct them to incorporate the clause into all contracts.⁵⁶ Second, DLA officials stated that the clause should be applied to all utilities privatization contracts so that there was consistency across the program. Since the issuance of the DLA contracting guidance in 2015, DLA officials stated that they have provided direction to the utilities privatization contracting officers on multiple occasions to incorporate the clause into all contracts and plan to ensure that the remaining contracts are modified to include the clause. DLA officials stated that most of the contract modifications to include this clause were completed in 2015 and 2016; however, some modifications occurred as late as 2017.⁵⁷

- *Army*: Army officials who manage the Army's other utilities privatization contracts stated that the clause requiring the

⁵⁴As we previously stated, DLA works with the military departments to plan for utility privatization and procures and administers utilities privatization contracts for the Departments of the Army and Air Force from the pre-solicitation phase and into the post-award phase. According to Navy officials, the Department of the Navy administers its own utilities privatization contracts for Navy and Marine Corps installations.

⁵⁵Officials from the Defense Procurement and Acquisition Policy Office conducted a review in the first quarter of fiscal year 2015 and found that the clause to safeguard DOD covered defense information was included in 65 percent of new awards at that time. The director of the Defense Procurement and Acquisition Policy office stated that the office planned to monitor implementation quarterly moving forward. Subsequently, DLA issued a contracting instruction memorandum stating that to ensure compliance DLA would modify all applicable contracts with the clause to safeguard covered defense information. See Defense Logistics Agency Memorandum, *Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012—Safeguarding Unclassified Controlled Technical Information Clause Compliance* (June 29, 2015). See also, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, *Safeguarding Unclassified Controlled Technical Information Clause Compliance* (Feb. 25, 2015).

⁵⁶Defense Logistics Agency memorandum, *Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012—Safeguarding Unclassified Controlled Technical Information Clause Compliance* (June 29, 2015).

⁵⁷According to DLA officials, the Defense Federal Acquisition Regulation Supplement clause has been incorporated into the standard utilities privatization contract template since July 2015.

safeguarding of covered defense information has been added to some contracts, but could not state definitively that the clause was added to all of the utilities privatization contracts that the Army manages. Army officials stated that Army contracting guidance issued in 2015 did not specifically address utilities privatization; however, the guidance did require that the clause be added to several different types of contracts, including all contracts for programs where officials expect covered defense information to be furnished by the government or developed by the contractor, and contracts that were active in fiscal year 2016 and later, among other contracts, or provide a rationale for not including the clause.⁵⁸ Army officials stated that they did not know if their utilities privatization contracts contained covered defense information. However, Army officials determined that the guidance required the clause to be added to utilities privatization contracts because these contracts fell into the category of contracts that were active in fiscal year 2016 and later. Another contracting officer for several Army privatization contracts stated that he does not recall how information about the guidance to incorporate the clause into utilities privatization contracts was shared. However, he stated that the issue was discussed at utilities privatization meetings, and he believed that it was implied at these meetings that the clause should be incorporated into existing utilities privatization contracts.

- *Air Force*: The Air Force official who manages the Air Force's utilities privatization program stated that two of the nine contracts managed by the Air Force included the clause, and the clause was being added to two additional contracts at the time of our review. Further, the Air Force stated that it was planning on adding the clause to the remaining five contracts. An Air Force official stated that it was not clear whether the clause was required to be incorporated into all existing utilities privatization contracts. However, since DLA added the clause across all of the utilities privatization contracts it managed, the Air Force official assumed that all non-DLA managed utilities privatization contracts should do the same.

⁵⁸Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology Memorandum, *Safeguarding Unclassified Controlled Technical Information*, (Apr. 30, 2015). In addition to the types of contracts listed above, the memorandum stated that the clause also needed to be added to programs designated as major defense acquisitions and other non-major acquisitions the advisory and assistance service contracts associated with these acquisition programs; and contracts for pre-acquisition category technology projects. Alternatively, a rationale should be provided for not including the clause in the contracts.

- *Navy*: Navy officials stated that they have not taken steps to incorporate the requirement into any of their utilities privatization contracts. According to Navy officials, they have not added the cybersecurity clause to the Navy's utilities privatization contracts because they are waiting for guidance from ASD (EI&E) regarding whether the clause is necessary for all utilities privatization contracts and, if so, additional guidance on how to implement the clause.

DLA, Army, and Air Force officials stated that while they have taken steps to incorporate the clause requiring the safeguarding of covered defense information into many of their utilities privatization contracts, they have not begun to implement the cybersecurity requirement for those contracts. As previously discussed, DOD acquisition guidance states that the requiring activity, which in the case of utilities privatization contracts is the military departments, must identify what information is considered covered defense information and provide that information to the contractor. However, before officials can fully implement these requirements, they must first identify what information is considered covered defense information.

According to an ASD (EI&E) official, information residing on ICS associated with privatized utility systems could be considered covered defense information because it could be used by adversaries to gain insights into operations on installations or to conduct a cyberattack. For example, information about energy or other commodity usage, water or gas pressure in pipes, or the amount of chemicals that need to be added during water treatment processes might be useful information to an adversary seeking to disrupt operations on a military installation. In one example of a cyber incident on an ICS associated with the operation of a dam in New York, a threat actor repeatedly obtained information on the status and operation of the dam, including information about the water levels, temperature, and status of the gate that controls water levels and flow rates. This access would allow the attacker to remotely operate and manipulate the dam's gate. However, in this instance, the gate had been manually disconnected for maintenance at the time of the intrusion.⁵⁹ In another example, threat actors obtained control-level access to a water treatment ICS and altered settings that controlled the amount of chemicals used to treat tap water and water flow rates, disrupting water

⁵⁹The Public-Private Analytic Exchange Program, *Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions* (2017). Supervisory control and data acquisition (SCADA) systems are industrial control systems and are generally used to control dispersed assets using centralized data acquisition and supervisory control.

distribution. The activity triggered an alert within the ICS, notifying the water treatment utility to quickly identify and reverse the chemical and flow changes, largely minimizing the impact on customers. Had the threat actors been more familiar with the flow control system, the attack could have been far more consequential.⁶⁰

However, DLA officials stated that there are currently no procedures that state what, if any, information associated with utilities privatization contracts is considered covered defense information. DLA officials stated that they conferred with Army and Air Force officials, and DLA's own policy division, and reached out to ASD (EI&E) to obtain a clear definition on what information associated with DOD's utilities privatization contracts might be considered covered defense information.

DLA's efforts to obtain clarification from ASD (EI&E) on how to implement the clause for utilities privatization contracts began in 2016. For example, in 2016, DLA officials stated they met with ASD (EI&E) officials to discuss the issue of covered defense information specific to the utilities privatization program, discussing what, if any, information on ICS associated with privatized utilities should be identified as covered defense information. Further, DLA officials asked for procedures regarding what steps to take to evaluate a contractor's compliance with the provision. In addition, DLA officials asked privatized utilities system owners to conduct a self-assessment of the cybersecurity controls they currently use for their ICS. DLA officials stated that they provided this information to ASD (EI&E) to aid decision making on how to approach cybersecurity for these systems. However, DLA officials stated that they did not receive a clear response from ASD (EI&E). DLA officials stated that because there are no procedures that definitively state which, if any, utilities privatization-related information should be categorized as covered defense information, they have been unable to provide clear procedures to the utilities privatization contractors who must implement the clause to safeguard any such information. Moreover, according to DLA officials, some of the utilities privatization contractors were reluctant to modify the contract to incorporate the clause for safeguarding DOD covered defense information because it was unclear how it was to be implemented. Also, Navy officials stated that they have not yet incorporated the clause into any of their utilities privatization contracts because they are waiting for procedures from ASD (EI&E). In addition, DLA and military department

⁶⁰Ibid.

officials stated that the current costs associated with implementing the clause are unknown.

Standards for Internal Control in the Federal Government require management to evaluate security threats to information technology, which can come from both internal and external sources, and periodically review policies and procedures for continued relevance and effectiveness in addressing related risks.⁶¹ Information technology refers to processes that are enabled by technology, including ICS, which are computer-controlled systems that monitor or operate physical utility infrastructure, among other things. DLA and military department officials stated they have not begun to implement the requirements in the clause because they are waiting for ASD (EI&E) officials to issue procedures concerning how the military departments are to determine what, if any, covered defense information associated with utilities privatization contracts is provided or developed by the contractor in performance of the contract. Such procedures are needed to help the military departments and DLA take the appropriate steps to implement the defense acquisition regulation clause for their utilities privatization contracts and safeguard covered defense information. An ASD (EI&E) official acknowledged that specific procedures concerning how the military departments are to determine what, if any, information associated with utilities privatization contracts is considered covered defense information are lacking and the office plans to update the policies. However, at the time of our review, it was not clear what that guidance will require.

In the absence of a clear understanding of how to implement the clause requiring the safeguarding of covered defense information, both installation officials and some system owners reported having taken various actions to address and enhance the cybersecurity of ICS associated with privatized utility systems. For example,

- An Air Force installation official stated that he and an employee of the privatized utility system worked closely with the installation's office that handles cybersecurity and followed service guidance to try to ensure mitigation of risks to and the security of the ICS.⁶² For example, officials ensured that the ICS could not be accessed

⁶¹GAO-14-704G.

⁶²Air Force Guidance Memorandum 2017-32-01, *Civil Engineer Control System Cybersecurity* (Feb. 2, 2017). This Air Force guidance memorandum establishes cybersecurity policy for civil engineer-owned or operated industrial control systems.

remotely and that authorized users are required to use strong passwords. The Air Force official stated that the privatized utility system owner may be required to apply additional cybersecurity measures in the future, depending on what decisions are made regarding the provision to safeguard covered defense information.

- A Navy installation official stated that he had no knowledge of what, if any, cybersecurity practices the privatized utility system owner had implemented for the ICS it uses to help operate an electrical distribution system. However, an official from the privatized utility system owner stated that the company has adopted some cybersecurity practices, which have been audited by an independent organization for 3 of the last 4 years, and the company plans to make this a standard part of business operations.
- Army officials stated that the installation relies on the privatized utility system owner to employ industry practices for cybersecurity efforts. Officials from the privatized utility system owner stated that the company has robust cybersecurity practices and the ability to continuously monitor the system to detect any unusual activities.

While installation officials and some system owners reported having taken some steps to address and enhance the cybersecurity of ICS associated with privatized utility systems, the lack of procedures may result in uncertainty as to whether covered defense information across utilities privatization contracts is safeguarded by the military departments and DLA. As previously reported, vulnerabilities in ICS can be exploited by various methods, causing loss of data, denial of service, or the physical destruction of infrastructure.⁶³ Without procedures concerning how the military departments are to determine what, if any, covered defense information is provided to or developed by the contractor in the performance of the utilities privatization contract, the military departments and DLA may not be able to take steps to adequately and consistently protect DOD's information associated with utilities privatization contracts.

Conclusions

As of January 2017, the military departments have privatized over 600 utility systems, and the Army and the Air Force have plans to privatize more systems in the coming years. While the military departments have some types of information on their privatized utilities, they have not

⁶³[GAO-15-749](#).

tracked utilities privatization contract performance or developed measurable performance standards, as asked for in the *Standards for Internal Control in the Federal Government*. In addition, while military department officials stated that they have perceived improvements in utility system reliability since utilities privatization, the military departments have not used contractor-provided data to determine reliability trends over time. Without issuing guidance that requires the military departments and DLA to develop and implement metrics and measurable performance standards to track contract performance for future utilities privatization contracts and to develop similar guidance for current utilities privatization contracts, the department will lack information on the performance of utilities privatization contracts. As a result, ASD (EI&E), the military departments, and DLA may not be able to perform effective program management and oversight for these long-term utilities privatization contracts.

DOD officials stated that they have taken steps to incorporate the clause requiring the safeguarding of covered defense information into many of their utilities privatization contracts, but they have not begun to implement the cybersecurity requirement for those contracts. DLA, Army, and Air Force officials stated they have not begun to implement the cybersecurity requirement for those contracts that include the clause because ASD (EI&E) has not issued specific procedures regarding how the military departments are to determine whether covered defense information is provided to or developed by the contractor in the performance of the utilities privatization contract. The lack of procedures may result in uncertainty as to whether covered defense information across utilities privatization contracts is safeguarded by the military departments and DLA. As previously reported, vulnerabilities in ICS can be exploited by various methods, causing loss of data, denial of service, or the physical destruction of infrastructure.⁶⁴ Without procedures concerning how the military departments are to determine what, if any, types of information are considered covered defense information and are provided to or developed by the contractor in the performance of the utilities privatization contract, the military departments and DLA will not be able to adequately and consistently protect DOD's information associated with utilities privatization contracts.

⁶⁴[GAO-15-749](#).

Recommendations for Executive Action

We are making two recommendations to the Secretary of Defense.

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Energy, Installations, and Environment, in consultation with the military departments, issues guidance requiring the military departments and DLA to develop and implement performance metrics and measurable performance standards to track utilities privatization contract performance for future utilities privatization contracts, and develops similar guidance for current utilities privatization contracts. (Recommendation 1)

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Energy, Installations, and Environment (a) issues procedures concerning how the military departments are to determine what constitutes covered defense information and what, if any, of this information is provided to or developed by the contractor in the performance of utilities privatization contracts, and (b) takes appropriate steps to protect such information. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. In written comments, DOD concurred with both of our recommendations. DOD's comments are reprinted in their entirety in appendix II. DOD also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and the Secretaries of the military departments. In addition, the report is available at no charge on our website at <http://www.gao.gov>.

If you or your staff members have any questions about this report, please contact Brian Lepore 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 III.

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

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

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

Appendix I: Selected Characteristics of the Department of Defense's (DOD) Utilities Privatization Contracts Included in GAO's Review

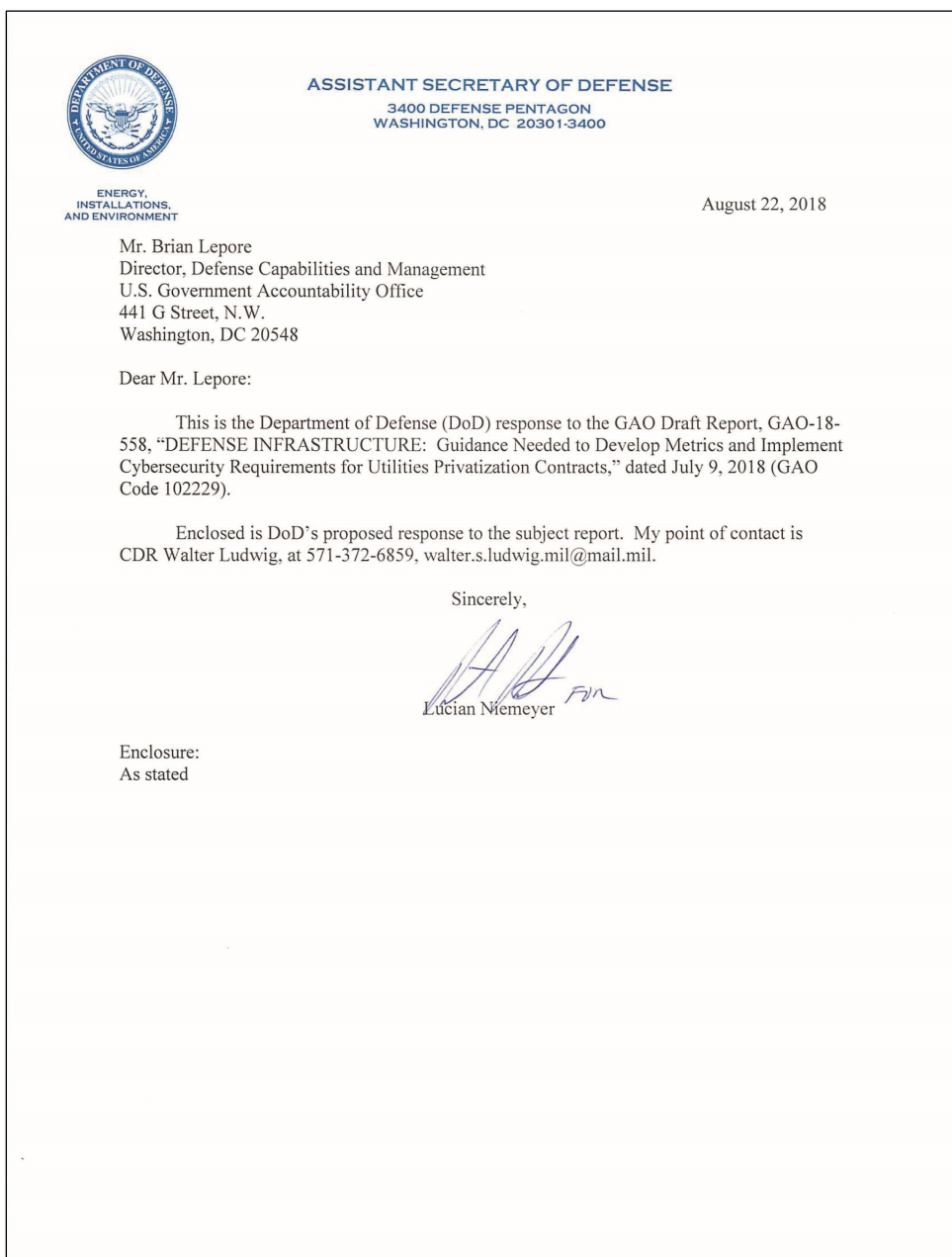
This appendix provides information on the nine utilities privatization contracts that we selected as case studies to review. Each of seven contracts privatized one utility system, and each of two contracts privatized two utility systems, for a total of 11 utility systems covered by the nine contracts. Table 2 lists selected characteristics of each contract.

Table 2: Selected Characteristics of the Nine Utilities Privatization Contracts Included in Our Review

Military Branch	Installation and location	Contract number	Date of award	Type of utility system privatized	Number of utility systems privatized
United States Army	Fort Bragg, North Carolina	SP0600-13-C-8284	9/26/2013	Natural Gas	1
	Fort Bragg, North Carolina	SP0600-07-C-8258	9/28/2007	Water & Wastewater	2
	Arlington National Cemetery, Virginia	SP0600-06-C-8251	9/15/2015	Electric	1
United States Air Force	Hill Air Force Base, Utah	SP0600-14-C-8291	6/12/2014	Electric	1
	Tyndall Air Force Base, Florida	SP0600-10-C-8254	9/17/2010	Natural Gas	1
	Tyndall Air Force Base, Florida	SP0600-10-C-8253	9/28/2010	Electric & Water	2
United States Navy	Naval Air Station Corpus Christi, Texas	N69450-08-C-0052	3/17/2008	Electric	1
	Naval Air Station Key West, Florida	N69450-07-C-0103	9/25/2007	Water	1
	Naval Air Station Key West, Florida	N62470-16-C-8000	10/26/2015	Wastewater	1

Source: GAO analysis of Department of Defense information. | GAO-18-558

Appendix II: Comments from the Department of Defense



GAO Draft Report Dated July 9, 2018
GAO-18-558 (GAO CODE 102229)

**“DEFENSE INFRASTRUCTURE: GUIDANCE NEEDED TO DEVELOP METRICS
AND IMPLEMENT CYBERSECURITY REQUIREMENTS FOR UTILITIES
PRIVATIZATION CONTRACTS”**

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

RECOMMENDATION 1: The Secretary of Defense should ensure that the Assistant Secretary of Defense for Energy, Installations, and Environment, in consultation with the military departments, issues guidance requiring the military departments and DLA to develop and implement performance metrics and measurable performance standards to track utilities privatization contract performance for future utilities privatization contracts, and develops similar guidance for current utilities privatization contracts.

DoD RESPONSE: The DoD concurs with this recommendation.

RECOMMENDATION 2: The Secretary of Defense should ensure that the Assistant Secretary of Defense for Energy, Installations, and Environment (1) issues procedures concerning how the military departments are to determine what constitutes covered defense information and what, if any, of this information is provided to or developed by the contractor in the performance of utility privatization contracts, and (2) takes appropriate steps to protect such information.

DoD RESPONSE: The DoD concurs with this recommendation.

Appendix III: 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, Kristy Williams (Assistant Director), Michael Armes, John Bauckman, Emily Biskup, Vincent Buquicchio, Carolyn Cavanaugh, Desiree Cunningham, Michael Gilmore, Simon Hirschfeld, Gina Hoover, Kush Malhotra, Richard Powelson, and Jack Wang made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Text of Appendix II: Comments from the Department of Defense

Page 1

Dear Mr. Lepore:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-18-558, "DEFENSE INFRASTRUCTURE: Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts," dated July 9, 2018 (GAO Code 102229).

Enclosed is DoD's proposed response to the subject report. My point of contact is CDR Walter Ludwig, at 571-372-6859, walter.s.ludwig.mil@mail.mil.

Sincerely,

Lucian Niemeyer

Enclosure:
As stated

Page 2

"DEFENSE INFRASTRUCTURE: GUIDANCE NEEDED TO DEVELOP METRICS AND IMPLEMENT CYBERSECURITY REQUIREMENTS FOR UTILITIES PRIVATIZATION CONTRACTS"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1:

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Energy, Installations, and Environment, in consultation with

the military departments, issues guidance requiring the military departments and DLA to develop and implement performance metrics and measurable performance standards to track utilities privatization contract performance for future utilities privatization contracts, and develops similar guidance for current utilities privatization contracts.

DoD RESPONSE:

The DoD concurs with this recommendation.

RECOMMENDATION 2:

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Energy, Installations, and Environment (1) issues procedures concerning how the military departments are to determine what constitutes covered defense information and what, if any, of this information is provided to or developed by the contractor in the performance of utility privatization contracts, and (2) takes appropriate steps to protect such information.

DoD RESPONSE:

The DoD concurs with this recommendation.

Related GAO Products

Defense Infrastructure: Actions Needed to Strengthen Utility Resilience Planning. [GAO-17-27](#). Washington, D.C., November 14, 2016.

Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning. [GAO-15-749](#). Washington, D.C., July 23, 2015.

GAO, Defense Infrastructure: Actions Taken to Improve the Management of Utility Privatization, but Some Concerns Remain. [GAO-06-914](#). Washington, D.C.: September 5, 2006.

Defense Infrastructure: Management Issues Requiring Attention in Utility Privatization. [GAO-05-433](#). Washington, D.C.: May 12, 2005.

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 (<https://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 <https://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, <https://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 <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548