THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION
AND SUSTAINMENT

FEB - 7 2019

MEMORANDUM FOR ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS, ENERGY AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE NAVY (ENERGY, INSTALLATIONS AND ENVIRONMENT)
ASSISTANT SECRETARY OF THE AIR FORCE (INSTALLATIONS, ENVIRONMENT AND ENERGY)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Supplemental Guidance for the Utilities Privatization Program

As captured in the National Defense Strategy, the variety and velocity of global threats continues to rapidly evolve. It is now undeniable that the homeland is no longer a sanctuary and that potential attacks against our critical defense, government, and economic infrastructure must be anticipated and mitigated. Maintaining access to reliable, resilient, and cybersecure energy resources, generation assets, distribution infrastructure, and facility-related controls and data is critical to the Department of Defense (DoD) mission execution.

Utilities privatization is one of several methods that a Service may use to finance utility improvements in support of the Department's energy reliability, energy resilience, and cybersecurity goals. In the privatization process, military installations shift from the role of owner-operators to that of smart utility service customers. As smart customers, it is incumbent upon DoD components to ensure that privatized utilities continue to support mission assurance goals and that requisite managerial and contractual controls are in place to ensure a ready force.

This memorandum and attachments one through four implement elements of the National Defense Strategy with a nexus to the Utilities Privatization Program. Additionally, they incorporate provisions from the National Defense Authorization Acts for Fiscal Years 2018 and 2019, which amend title 10, United States Code, section 2688 requiring privatized systems be operated in a manner consistent with energy resilience and cybersecurity requirements and metrics. This guidance supersedes enclosure 3, section 3e. Utilities Privatization of DoD Instruction 4170.11, "Installation Energy Management," change 1, effective March 16, 2016, and cancels Under Secretary of Defense for Acquisition, Technology, and Logistics Memoranda, "Supplemental Guidance for the Utilities Privatization Program" of March 20, 2006, and "Supplemental Guidance for the Utilities Privatization Program" of September 20, 2010, and will expire at such time as formally incorporated into an authoritative revision of that Instruction.

In accordance with 10 U.S.C. 2688(d)(2) and subject to the provisions of this guidance, the Secretaries of the Military Departments are authorized to determine the cost effectiveness of a contract for utility services for a term not to exceed 50 years. This authority may not be redelegated below the level of an assistant secretary.

The DoD Components shall take immediate action to implement the procedures outlined in this supplemental guidance. My point of contact is Mr. Walter Ludwig. He can be reached at 571-372-6859.

Ellen M. Lord

Attachment:
As stated

ATTACHMENT (1) - REFERENCES

(a) Public Law 110-140, "Energy Independence and Security Act of 2007," December 19, 2007
(b) Public Law 109-58, "Energy Policy Act of 2005," August 8, 2005
(c) 10 U.S. Code § 101 - Definitions
(d) 10 U.S. Code § 2688 - Utility Systems: Conveyance Authority
(e) 10 U.S. Code § 2925 - Annual Department of Defense energy management reports
(f) Executive Order 13221, "Energy Efficient Standby Power Devices," July 31, 2001
(g) OMB Circular A-94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs," October 29, 1992
(h) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998 DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014
(i) DoD Directive 4140.25, "DoD Management Policy for Energy Commodities and Related Services," April 12, 2004 June 25, 2015 Sections 8251 et seq. and 6361 et seq. of title 42, United States Code
(j) DoD Directive 4180.01, "DoD Energy Policy," April 16, 2014
(k) DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016
(l) DoD Instruction 4170.11, "Installation Energy Management," Change 1, Effective March 16, 2016
(m) DoD Instruction 6055.17, "DoD Installation Emergency Management (IEM) Program," January 13, 2009
(n) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(o) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
(p) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network (DODIN) Operations," March 7, 2016
(q) Unified Facilities Criteria (UFC) 4-010-06, "Cybersecurity of Facility-Related Control Systems (FRCS)," September 30, 2015
(r) Deputy Assistant Secretary of Defense for Logistics Memorandum, "Department of Defense Energy Security Policy," January 14, 1992
(s) "Department of Defense Energy Manager's Handbook," August 25, 2005
(t) Deputy Undersecretary of Defense Energy Installations and Environment (DUSD (I&E)), "Power Resilience Review Memorandum," December 16, 2013
(u) Office of Deputy Assistant Secretary of Defense Energy Installations and Environment (ODASD (EI&E)), "Energy Resilience: OM&T Strategy and Implementation Guidance Memo," March 17, 2017
(v) Assistant Secretary of Defense Energy Installations and Environment (ASD (EI&E)), "Managing Cyber Risks to Facility-Related Control Systems," March 31, 2016

(w) Assistant Secretary of Defense Energy Installations and Environment (ASD (EI&E)), "Installation Energy Plan," March 31, 2016
(x) DoD Federal Acquisition Regulations Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."
(y) DFARS 252.227-7013, Rights in Technical Data—Noncommercial Items
(z) NIST Special Publication (SP) 800-171 Rev 1, "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations," December 2016 (updated 2/20/2018)
(aa) DoD Mission Assurance Assessment benchmarks, March 28, 2018
(bb) Defense Threat Reduction Agency DoD mission Assurance Assessment Guidelines, March 29, 2018
(cc) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Supplemental Guidance for the Utilities Privatization Program," March 20, 2006 (hereby cancelled)
(dd) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Supplemental Guidance for the Utilities Privatization Program", September 20, 2010 (hereby cancelled)

ATTACHMENT (2) – POLICY AND PROCEDURES

I. PURPOSE

Implement elements of the National Defense Strategy with a nexus to the Utilities Privatization Program. Expand upon, update and revise guidance provided by references (a) through (dd) of Attachment (1). Address changes to 10 U.S.C. 2688. Provide guidance to the Department of Defense (DoD) Components on implementation of the Utilities Privatization Program while interim DoDI 4170.11 updates are being adjudicated.

II. POLICY

The National Defense Authorization Acts for Fiscal Years 2018 and 2019 made several changes to 10 U.S.C. 2688 including the requirement that privatized utilities shall be operated in a manner consistent with energy resilience and cybersecurity requirements and metrics. Additionally, the Secretary of Defense has issued instructions and guidance via references (h) through (dd) of Attachment (1) requiring that DoD Components take the necessary steps to ensure that installation energy assets are managed in accordance with DoD energy resilience and cybersecurity objectives, requirements, and metrics. To ensure adequate security of how utility data is processed, stored, or transmitted on a privatized system owner's internal network, utility data will be handled as Covered Defense Information (CDI)/ Controlled Unclassified Information (CUI). Utility data is all types of data, as defined in Attachment (3), required to provide privatized utility services.

As of the date of this memorandum, reference (l) is in the process of update and adjudication. In the interim, the following guidance is being provided to assist the DoD Components in implementing the Utilities Privatization Program. This guidance supersedes *Enclosure 3, Section 3e., Utilities Privatization,* of reference (l) above and will expire at such time as formally incorporated in an authoritative revision.

A. Background

Historically, military installations have been challenged to maintain reliable utility systems that keep pace with operational and mission needs. Additionally, evolving energy resilience and cybersecurity requirements are placing increasing financial and operational demands on those same systems. Reference (w) provides a framework through which military installations integrate applicable installation and higher level strategic guidance into a comprehensive energy roadmap that addresses energy needs in an integrated and cost-effective manner.

Reference (l) provides DoD policy on a variety of appropriated funded and alternatively financed solutions that may be used by DoD Components to improve utility and building infrastructure. Alternative Financing Mechanisms (AFMs) leverage commercial sources of capital in order to finance near-term enhancements to DoD utility infrastructure. As part of a comprehensive Installation Energy Plan (IEP), AFMs can provide material benefits to DoD Components by providing cost-effective access to capital that might not otherwise have been obtainable through traditional methods. AFMs require DoD

Components, however, to also use contractual mechanisms to ensure compliance with energy security, energy resilience, and cybersecurity requirements.

Utilities privatization is one of several AFMs that a Military Department may use to finance utility improvements in support of the DoD's energy reliability, energy resilience, and cybersecurity goals. Except where the Secretary of a Military Department has certified that a system is exempt due to security reasons or where privatization is uneconomical, a Military Department may privatize a utility system owned by the United States at an Active or Reserve Component installation within and outside the United States that is not designated for closure under a base closure law or subject to a public-private competition under 10 U.S.C. 2461. In the privatization process, military installations shift from the role of owner-operators to that of smart utility service customers.

Privatized systems continue, however, to function as Defense Critical Infrastructure (DCI) in accordance with reference (k) and a DoD Component's decision to pursue utilities privatization must be consistent with prioritized mission assurance requirements, 10 U.S.C. 2688, applicable DoD instructions and guidance, and the affected installation's IEP.

B. Pre-conveyance Requirements, Planning, and Analysis

1. Business Case Analysis

In accordance with paragraph (d) of reference (d), Military Departments as designees of the Secretary of Defense must develop a Business Case Analysis (BCA) that supports any proposed utility service contract that has a term in excess of 10 years. The BCA must analyze both qualitative and quantitative factors and must comprehensively document the level of investment required to maintain adequate operation of the utility system over the proposed term of the contract. Specifically, the BCA must document how privatization and the related utility service contract support the DoD Component's mission assurance, energy resilience, and cybersecurity requirements. In formulating the independent estimate of the level of investment required, the BCA shall address all costs needed to ensure that the conveyee manages and operates the utility system in a manner consistent with energy resilience and cybersecurity requirements and associated metrics including those costs related to metrics tracking and reporting in accordance with 10 U.S.C. 2925(a) and other requirements as defined by the Secretary of Defense. Prior to entering into any utility service contract in excess of 10 years, the Secretary of the Military Department concerned shall submit the associated BCA to the Secretary of Defense for oversight review. The Secretary of Defense shall have a minimum of 10 business days to complete its review before further action is taken on the contract action by the Military Department.

2. Energy Resilience

As defined in reference (c), the term "energy resilience" means the ability to avoid, prepare for, minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness, including mission essential operations related to readiness,

and to execute or rapidly reestablish mission essential requirements. Reference (l) requires DoD Components to take necessary steps to ensure resilience on military installations and reference (d) requires that the Secretary concerned shall include in any contract for the conveyance of a utility system (or part of a utility system) that the conveyee manage and operate the utility system in a manner consistent with energy resilience requirements and metrics provided to the conveyee to ensure that the reliability of the utility system meets mission requirements. As appropriate, conveyees shall operate, maintain, and test applicable energy generation systems, infrastructure, and equipment in a manner that meets the requirements of reference (u) over the contract term. At a minimum, the BCA required in section B1 must address the proposed framework through which energy resilience requirements will be implemented, monitored, and, as necessary, amended over the contract term.

3. Cybersecurity

DoD recognizes the risk posed by emerging threats to its mission critical cyber-supported Facility Related Control Systems (FRCS). FRCS cybersecurity enables resilience of essential utilities and other key services that support mission requirements. Utility system owners are accountable for system operational resilience and cybersecurity, including the safeguarding of CDI related to utility services.

DoD Components shall ensure that new and existing utility service contracts incorporate comprehensive cybersecurity requirements as outlined in the references (h) through (y) of Attachment (1) to ensure that FRCS and networks are both physically and logically cybersecure. Effective immediately, the DoD Components shall incorporate references (x) to (bb) in all new or renewing utility service contracts, or contracts undergoing material modifications or price redeterminations. Additionally, no later than sixty (60) days after the issuance of this guidance, the DoD Components shall submit a plan to the Office of the Assistant Secretary of Defense for Sustainment (ASD(S)) for review and approval documenting how references (x) to (bb) will be incorporated into existing utility service contracts. DoD Components shall provide updates to the ASD(S) on the status of the implementation of the incorporation of references (x) to (aa) during the Component's Annual Portfolio Program Review.

4. Performance Metrics, Measures, and Requirements

The Secretary of Defense has directed the DoD to focus its institutional effort on producing tangible warfighter achievements versus performing perfunctory activities. DoD Components shall develop correlated, outcome-oriented performance metrics and measures to implement and manage their utility service contracts in order to meet economic, utility reliability, energy resilience, and cybersecurity requirements.

Minimum metrics, measures, and requirements are listed in the following table:

Measurement Area	Metric / Measure/ Requirement
Economic	• Plant replacement value (at time of conveyance) • Cost control • Energy savings and efficiencies (if any)
Utility Reliability	• System availability o Planned versus unplanned outages • Reliability response time • Condition assessment (life safety) • Inventory changes
Energy Resilience	Mission Availability* = $\frac{\text{Uptime}^{**}}{\text{Uptime} + \text{Downtime}^{***}}$ **This metric does not constitute a "system" availability metric, rather it should represent a mission requirement (critical load) that identifies an energy capability metric. Uptime and Downtime shall be measured at the critical asset level vice the utility system level (see next lines for definitions of Uptime and Downtime)* *** Uptime is length of time the critical mission operation requires energy throughout the year* **** Downtime is a risk-based metric used to determine how much allowable downtime the critical mission operation can tolerate before mission failure occurs*
Cybersecurity	• All FRCS on separate segmented and secure network • All FRCS being continuously monitored (IAW Risk Management Framework (RMF) compliance schema detailed in FRCS Cybersecurity Plan Guidance) • All FRCS registered in Enterprise Mission Assurance Support System (eMASS) or alternative equivalent repository • Cyber Risk Management Plan (CRMP) or other report format of implementation of reference (y) IAW reference (x) • Plan for risk mitigation and identification of non-compliant components and devices (i.e., legacy systems that require replacement to meet current generation capabilities)

The DoD Components shall document the method and frequency by which metrics and measures will be gathered, monitored, analyzed, and reported. DoD Components at a minimum must establish baseline metrics at the inception of privatization actions in order to quantitatively produce a framework for comprehensive continuous improvement, monitoring,

and reporting. If a military installation does not have historical metrics, it may require the privatization contractor to use data from the first year of privatized operations to establish a baseline.

5. Economic Analysis

The DoD Components shall perform an Economic Analysis (EA) as part of the BCA documenting the level of investment required to maintain adequate operation of the utility system over the proposed term of the contract. The EA should demonstrate how the economic case for privatization achieves DoD's mission assurance, energy reliability, energy resilience, and cybersecurity requirements at an effective life cycle cost. An EA should be informed by outputs from a Component's IEP (reference (w)). Specifically, in phase 3 of an IEP, military installations conduct an analysis of promising project alternatives in order to incorporate a balance of energy production, distribution infrastructure, and demand reduction activities that will meet their mission critical energy requirements at the lowest life cycle cost. Outputs from this analysis should be included in the UP EA to provide context for a determination of comparative life cycle cost effectiveness. The EA shall also consider the economic impacts of the value of money, the cost of borrowing, and the impact of taxes (including those related to Contribution in Aid of Construction (CIAC)).

Paragraph (d) of reference (d) requires the Secretary of Defense, or designee, to make an assessment of cost effectiveness in approving utility service contracts with terms in excess of 10 years. The Secretary of the Military Department concerned shall report to the Secretary of Defense those proposed privatization actions in which the long-term costs to the United States of utility services provided by the utility system will not be at least ten percent less than the long-term cost for provision of those utility services in the agency tender. The term "agency tender" refers to the Government's "should-cost estimate." The DoD Components shall report the qualitative and quantitative mission assurance and national defense benefits obtained in relationship to the variance in cost from the ten percent threshold. The DoD Components must ensure that comprehensive life cycle costs are included in the EA, including those costs necessary to ensure compliance with energy reliability, energy resilience, and cybersecurity requirements. The BCA must also assess the continuing cost of managing the metrics and measures framework from paragraph B4 above. Since the Military Departments may not dispose of the Government's property without receiving an appropriate return, the consideration for the sale of the utility system must include evaluation of the value of system itself (which should be calculated applying rules governing CIAC taxes) and any right-of-way granted to the new owner. The DoD Components must use an EA tool approved by OSD for all privatization decisions.

C. Post-Conveyance Contract Administration

A Post-Conveyance Contract Administration Plan shall be developed for each privatized utility. DoD Components shall ensure that BCA quantitative and qualitative elements supporting the case for privatization are sufficiently protected and incorporated into any resultant utility service contract. The Plan shall specifically address the method and manner by which energy reliability, energy resilience, and cybersecurity metrics and measures

will be gathered, monitored, analyzed, and reported to effectuate positive mission assurance outcomes. As noted in paragraph B4 above, metrics and measures shall be evaluated and analyzed over time to identify trends for predictive analysis and decision making and to foster a quantitative framework for risk management and continuous improvement.

1. Post Conveyance Reviews

The National Defense Strategy outlines the budget discipline and affordability required to achieve solvency and improve readiness. Cost growth must be monitored and managed in order to balance performance and affordability. Recognizing the value of comparing projected to actual costs, DoD Components shall conduct a Post Conveyance Review (PCR) of each privatized system. To ensure its value, a review shall be conducted within 2 to 3 years after award or 1 year after the first price re-determination, whichever is later, and no later than every 10 years thereafter until contract expiration. These timeframes allow for proper contractor transition and steady state operation. No later than ninety (90) days after the issuance of this guidance, the DoD Components shall submit to the ASD(S) for approval a time-phased Post Conveyance Review Implementation Plan (PCRIP) for each new and existing privatized system. DoD Components shall prioritize installations identified by the Office of the Deputy Assistant Secretary of Defense for Defense Continuity and Mission Assurance as well as existing privatized systems that have not completed PCRs in compliance with reference (l). DoD Components shall complete PCRs for at least 50% of all privatized systems within 5 calendar years of the ASD(S) approval date of their PCRIP. DoD Components shall complete remaining PCRs within 10 calendar years of the ASD(S) approval date of their PCRIP.

A PCR shall include, at a minimum, a joint detailed inventory, an updated list of requirements reflecting changes, an updated list of transition requirements (to include compliance with reference (y) IAW reference (x), an 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, and any unintended benefits/costs. Costs shall be summed over the period from award to analysis and compared to projections. Record of the original Government estimate and contract cost shall be maintained throughout the life cycle of the contract. Contract cost shall be normalized to the inflation factors in the Government estimate and adjusted for any changes in mission or regulatory environment.

The PCR shall also provide an assessment of the ability of the privatized system to meet the DoD Component's requirements for energy reliability, energy resilience, and cybersecurity. At a minimum the review shall include quantitative trend analyses of metrics and measures from paragraph B4, input from affected mission assurance, public works, information technology, and installation stakeholders, as well as an actionable plan to correct any deficiencies identified during the review.

All analysis results shall be maintained throughout the life of the service contract. Data from the PCR will be maintained for historical and predictive analysis of the challenges and successes of UP. ASD(S), at its discretion, may choose to participate as an observer in the Military Department's PCR or independently perform an ex post analysis of a Military

Department's review. At a minimum, ASD(S) will independently perform at least one review per DoD Component per year.

2. Cost Growth Control

Once a utility system has been privatized, the Government must enter into sole source negotiation with a single provider for any changes in inventory and service price. It is imperative that DoD Components be cost informed in their management of utility service contracts in order to strike the right balance between mission assurance needs and finite fiscal resources.

DoD Components shall establish a cost baseline for each privatization action documenting recurring costs and inventory levels once an initial steady state is achieved or by year six of the privatization contract, whichever is earlier. Typically, steady state operations are attained in the first five years of the utility service contract allowing for changes in initial inventory estimates, changes in site conditions, capital upgrades, and other site-specific requirements. Cost growth shall be formally monitored by the DoD Components through PCRs and Cost Growth Reviews (see following paragraph). If cost growth in excess of 20% of the initial privatization cost baseline is found during either of these reviews, the DoD Component shall submit a Cost Control Report to ASD(S) within 90 days of discovery documenting the reasons for cost variance as well as corrective actions it will take to mitigate cost risk.

Post Conveyance Reviews will readily identify cost growth not associated with normal increases in inventory or price indices. This information will place the Government in a better position to negotiate the future contract price. In addition to PCRs, DoD Components shall conduct phased Cost Growth Reviews on at least 20% of their privatized portfolio per year such that all systems are reviewed at least once on a repeating five-year cycle. In the case where the PCR is on the same cycle as the Cost Growth Review, one report which is inclusive of the requirements for both may be submitted. Summary findings of both PCRs and Cost Growth Reviews shall be presented by the DoD Component to ASD(S) at the Annual UP Program Review described in Article D below.

D. Annual UP Program Review

ASD(S) will conduct an annual UP Program Review with each DoD Component to address portfolio lessons learned, identify opportunities for policy level improvements, and assess the UP Program's continuing warfighter value proposition. Annual reviews will specifically address the Program's ability to cost effectively support mission assurance, energy reliability, energy resilience, and cybersecurity requirements.

E. Reporting:

The DoD Components shall report the following:

1. Pre-conveyance BCA for all conveyance decisions 30 days prior to conveyance award
2. UP 5-year plan by January 1st of each year
3. PCRIP time phased by fiscal year by October 31st
4. Summary report of Operations Maintenance & Testing (OM&T) compliance IAW reference (u) including any deficiencies and remedies planned/implemented as outlined in the "accepted reports" section of said guidance
5. Cybersecurity reporting: UP annual self-attestation of cyber risk management plan in compliance with NIST 800-171 or a Defense Contracting Audit Agency (DCAA) or Defense Logistics Agency (DLA) audit verifying compliance. Reporting of compliance of UP self-attestation will be accomplished via the annual UP database update
6. Portfolio level items at Annual UP Program Review

ATTACHMENT (3) - PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Executive Order 13556 "Controlled Unclassified Information" 2010

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Executive Order 13556 "Controlled Unclassified Information" (the Order), establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).

32 CFR Part 2002 "Controlled Unclassified Information" was issued by ISOO to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the Program. The rule affects Federal executive branch agencies that handle CUI and all organizations (sources) that handle, possess, use, share, or receive CUI—or which operate, use, or have access to Federal information and information systems on behalf of an agency.

CUI Categories and Subcategories

Twenty-two categories of CUI data are defined by the National Archives and Records Administration (NARA), of which five are pertinent to the Installations and Environment community and related to the Critical Infrastructure Category: Controlled Technical Information, Critical Infrastructure, DoD Critical Infrastructure Security Information, Critical Energy Infrastructure Information, Physical Security, and Protected Critical Infrastructure Information.

Category-Subcategory: Controlled Technical Information

Category Description: Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical

Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Subcategory Description: N/A

Marking: CTI

Category-Subcategory: Critical Infrastructure

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: N/A

Marking: CRIT

Category-Subcategory: Critical Infrastructure-DoD Critical Infrastructure Security Information

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated on behalf of the DoD, including vulnerability assessments prepared by or on behalf of the DoD, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.

Marking: DCRIT

Category-Subcategory: Critical Infrastructure-Critical Energy Infrastructure Information

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public

health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that: (i) Relates details about the production, generation, transportation, transmission, or distribution of energy; (ii) Could be useful to a person in planning an attack on critical infrastructure; and (iii) Does not simply give the general location of the critical infrastructure.

Marking: CEII

Category-Subcategory: Critical Infrastructure-Physical Security

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: Related to protection of federal buildings, grounds or property.

Marking: PHYS

Category-Subcategory: Critical Infrastructure-Protected Critical Infrastructure Information

Category Description: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.

Subcategory Description: As defined by 6 USC 131-134, and 6 CFR 29, PCII relates to threats, vulnerabilities, or operational experience related to the national infrastructure. PCII offers protection to private sector infrastructure information voluntarily shared with government entities for purposes of homeland security.

Marking: PCII

ATTACHMENT (4) - ACRONYMS AND ABBREVIATIONS

AFM	Alternative Financing Mechanism
ASD(EI&E)	Assistant Secretary of Defense, Energy Installations and Environment
ASD(S)	Assistant Secretary of Defense, Sustainment
BCA	Business Case Analysis
CDI	Covered Defense Information
CIAC	Contribution in Aid of Construction
CRMP	Cyber Risk Management Plan
CUI	Controlled Unclassified Information
DCAA	Defense Contracting Audit Agency
DCI	Defense Critical Infrastructure
DLA	Defense Logistics Agency
DoD	Department of Defense
EA	Economic Analysis
eMASS	Enterprise Mission Assurance Support System
FRCS	Facility Related Control Systems
IAW	In accordance with
IEP	Installation Energy Plan
NARA	National Archives and Records Administration
OM&T	Operations Maintenance & Testing
PCR	Post Conveyance Review
PCRIP	Post Conveyance Review Implementation Plan
RMF	Risk Management Framework
UP	Utilities Privatization