COMMENTS OF THE EDISON ELECTRIC INSTITUTE ON THE DEPARTMENT OF DEFENSE, DEFENSE ACQUISITION REGUALTIONS SYSTEM INTERIM RULE TO AMEND THE DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT TO IMPLEMENT AN ASSESSMENT METHODOLOGY AND CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK

DOCKET NO. DARS-2020-0034

November 30, 2020

The Edison Electric Institute (EEI) appreciates this opportunity to respond to the Department of Defense's (DoD's) interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification (CMMC) framework for assessing contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. *85 Fed. Reg. 61,505* (Sept. 29, 2020).

The interim rule adds a new DFARS subpart, Subpart 204.75, Cybersecurity Maturity Model Certification (CMMC), to specify the policy and procedures for awarding a contract, or exercising an option on a contract, that includes the requirement for a CMMC certification. Specifically, this subpart directs contracting officers to verify in the Supplier Performance Risk System that the offeror's or contractor's CMMC certification is current and meets the required level prior to making the award. The interim rule provides two mechanisms to assess a contractor's implementation of the DOD's cybersecurity requirements moving forward: (1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology, which outlines the assessment of a contractor's SP 800-171 implementation, as required by DFARS clause 252.204 - 7012, Safeguarding Covered Defense Information and Cyber Incident Reporting; or (2) the CMMC framework, which builds on the

800–171 Assessment Methodology by adding a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. The CMMC framework is designed to provide increased assurance to DoD that a contractor can adequately protect sensitive unclassified information such as Federal Contract Information and, notably, Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans and operate in all 50 states and the District of Columbia. These customers include various DoD facilities under various arrangements, including situations in which electric infrastructure formerly owned and operated by the military has been transferred to investor-owned electric companies and other utilities. Such arrangements have been determined by DoD to be economic and in the best interests of national security because they ensure these systems are operated and maintained to industry standards. As of December 2019, DoD had privatized 614 of 2,590 utility systems on military installations worldwide.[1] DoD intends to continue to transfer ownership and operation of utility services to military installations. EEI's members are committed to providing affordable, reliable, and clean electricity to customers now and in the future.

EEI and its member companies support the national security goals of the interim rule. Knowing that sophisticated adversaries target exploitable vulnerabilities with the intent to attack the electric grid, EEI members look forward to working with DoD to understand how to

[1] *See* Government Accountability Office, *DOD Utilities Privatization: Improved Data Collection and Lessons Learned Could Help Reduce Time to Award Contracts*, GAO-20-104 (Apr. 2020), https://www.gao.gov/assets/710/705669.pdf.

implement the security requirements of the assessment methodologies.

Electric companies use a variety of tools in combating cybersecurity threats to the grid. In this light, EEI provides feedback to DoD to highlight issues that are uniquely applicable to the electric sector and urges DoD to consider the importance of electric system reliability to national security as it implements the interim rule and engages in the assessment methodologies.

I. COMMENTS

Electric companies engage in many activities and use multiple tools to protect the electric grid from malicious cyber attacks, and the current tools and processes complement the goals that DoD is seeking to achieve. Collectively, electric companies engage in activities that underscore the seriousness with which they take the importance of providing continuous, reliable and resilient operation of the electric grid. Electric companies undertake considerable and varied measures to protect their systems and supply chains form malicious cyber attacks. EEI member electric companies take a risk-based, defense-in-depth philosophy and use corresponding tools that are integrated in electric companies' security culture. In addition, electric companies face unique threats due to their location, size, system design and topology, customer base and security controls. This multi-layered approach encompasses compliance with rigorous, mandatory, and enforceable reliability standards and regulations developed by the North American Electric Reliability Corporation and enforced by the Federal Energy Regulatory Commission. The approach also includes activities that surpass the minimum regulatory requirements and extends to close coordination among industry and with government partners at all levels. This includes (1) deploying technologies that improve situational awareness; (2) ensuring threat indicators are communicated at the right time to the right people in industry and government; (3) preparing for and exercising coordinated responses to malicious threats to energy grid operations; and (4)

working closely with other interdependent infrastructure sectors (communications, downstream natural gas, financial services, and water) to enhance preparation and response to threats against the grid. EEI would welcome engagement with DoD to elaborate on our members' unique environment as well as challenges electric companies face as government contractors providing electricity to key government facilities.

In the interim rule, DOD states that the CMMC is designed to provide increased assurance to DoD that a contractor can adequately protect sensitive unclassified information, notably CUI at a level commensurate with the risk. The DoD also states in the interim rule that the CMMC model encompasses the security requirements for CUI specified in NIST SP 800-171. NIST SP 800-171 provides federal agencies with recommended security requirements for protecting the confidentiality of CUI: (1) when the CUI is resident in a non-federal system and organization; (2) when the non-federal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category. The requirements apply only to components of non-federal systems that process, store, or transmit CUI, or that provide security protection for such components. The requirements are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. NIST SP 800-171 also states that the protection of unclassified federal information in non-federal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies, and notes Executive Order 13556, which established a government-wide definition of CUI to standardize the way the executive branch

handles unclassified information that requires protection. Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI. Thus, in general, any unclassified information that requires safeguarding or dissemination control is CUI. *See* 32 C.F.R. part 2002.

CUI is geared toward how federal agencies and departments define CUI. This poses unique challenges for the electric sector. To address these challenges, further clarification of how DoD intends to identify CUI is needed. It is difficult for electric companies to identify information systems that are processing, storing or transmitting CUI. The electric sector needs the government to provide a clear and consistent definition of CUI to effectively implement the rule. For example, clarification about what information on an electric company's information system is deemed to be "government created or owned unclassified information" is needed. Electric companies have a great deal of experience in protecting systems and information from unauthorized but need further guidance from DoD.

EEI looks forward to working with DoD to understand the unique electric company challenges faced by the implementation of the interim rule and to avoid unintended harm to the electric power industry.