DR. JENNIFER L. UHLE
Vice President, Generation and Suppliers

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8164
jlu@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

May 21, 2021

Mr. Michael Coe
Director, Energy Resilience Division of the Office of Electricity
Mailstop OE–20, Room 8H–033
Department of Energy
1000 Independence Avenue SW
Washington, DC
20585

Subject: Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure [April 22, 2021]

Dear Mr. Coe,

The Nuclear Energy Institute (NEI)[1], on behalf of its members, is pleased to respond to the Department of Energy's (DOE) April 22, 2021, Request for Information (RFI).[2] The April RFI was issued pursuant to Executive Order 13990, "Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis," (EO 13990) and seeks information potentially relevant to the nation's critical electric infrastructure. The RFI is part of a broader government initiative to enhance the integrity and security of priority sites' control systems and to develop a strengthened approach to address the supply chain security of the U.S. electricity subsector.

NEI and its member companies support the broad national security goals of EO 13990. We believe that the current regulatory framework applicable to nuclear energy generation facilities in areas like cyber security and quality assurance provides robust protection of the safety-related structures, systems, and components

[1] The Nuclear Energy Institute (NEI) is responsible for establishing unified policy on behalf of its members relating to matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect and engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations involved in the nuclear energy industry.

[2] "Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure," 86 Fed. Reg. 21309 (April 22, 2021).

(SSCs) that are vital to the safe operation of nuclear energy facilities. These requirements, coupled with the industry's substantial, regulator-approved programs in these areas, also contribute to the resilience and reliability of the nation's nuclear power generation facilities. As discussed below, the applicable regulatory framework is the culmination of extensive interactions between the Federal Energy Regulatory Commission (FERC) and the U.S. Nuclear Regulatory Commission (NRC) that date back to at least the early-2000s.

The FERC and the NRC both have responsibilities to ensure that the nation's nuclear energy generating stations are protected from cybersecurity threats. FERC's requirements consist of the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) reliability standards. NERC's primary objective in developing and enforcing these standards is to ensure bulk power system (BPS) reliability. The NRC's cybersecurity requirements are contained in 10 CFR 73.54, "Protection of digital computer and communication systems and networks." The NRC's primary regulatory focus is to prevent "radiological sabotage (*i.e.*, significant core damage) that could result in harm to public health and safety or the environment or have an adverse impact upon the common defense and security."[3]

In 2011, the NRC determined as a matter of policy, that the NRC's cybersecurity regulation includes SSCs in the balance-of-plant (BOP) that "have a nexus to radiological health and safety at NRC-licensed nuclear power plants" (i.e., SSCs out to the first inter-tie with the offsite distribution system that could, if compromised, result in an unplanned reactor shutdown or transient).[4] These are the same SSCs at a nuclear plant that are important from a reliability perspective. Thus, the NRC's requirements cover digital systems that are either important for safety or for reliability.

The NRC's cybersecurity regulations require commercial nuclear generation facilities to provide robust protection from cyber threats. Specifically, each nuclear generating station's cybersecurity program must protect digital computer and communication systems and networks against cyber-attacks. The systems and networks subject to the NRC's cybersecurity requirements cover digital computer and communication systems and networks associated with:

- Safety-related and important-to-safety functions
- Security functions
- Emergency preparedness functions, including offsite communications
- Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions[5]

---

[3] "Final Memorandum of Understanding Between the U.S. Nuclear Regulatory Commission and the North American Electric Reliability Corporation," 75 Fed. Reg. 1416 (January 11, 2010) (NRC-NERC MOU).

[4] *See* Staff Requirements Memorandum (SRM)-COMWCO-10-0001, "Regulation of Cyber Security at Nuclear Power Plants," (Oct. 21, 2010). As defined in 10 CFR 170.3, the balance of plant "consists of the remaining systems, components, and structures that comprise a complete nuclear power plant and are not included in the nuclear steam supply system."

[5] 10 CFR 73.54(a)(1). Nuclear power plant licensees' physical protection programs must comply with the performance objectives and requirements outlined in 10 CFR 73.55, "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." Section 73.55(b)(8) requires these licensees to establish, maintain, and implement a cybersecurity program in accordance with Section 73.54. Incorporating a cybersecurity

The NRC requires commercial reactor licensees to protect these systems from cyber-attacks that would adversely impact the integrity or confidentiality of data and/or software; deny access to systems, services, and/or data; and adversely impact the operation of systems, networks, and associated equipment.[6] Commercial power reactor licensees implement these requirements through a cybersecurity plan that must be approved by the NRC and that is subject to NRC oversight, including regular inspections and, if necessary, enforcement action.[7] These plans provide tremendous defense-in-depth and lay out comprehensive cybersecurity programs that include air gapping systems, unidirectional security gateways or data diodes that allow data to travel in only one direction, use of tamper-proof devices, log reviews and additional technical, management, and operational controls. The NRC and the industry have issued detailed regulatory guidance to assist licensees in complying with the NRC's cybersecurity requirements.[8] Notably, NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," and NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," also addresses supply chain controls.[9]

In addition to the NRC's cyber security requirements, commercial nuclear power reactor licensees are also subject to stringent quality assurance requirements, which are set forth in Appendix B to 10 CFR Part 50, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants." These regulations require power reactor licensees to implement an NRC-approved Quality Assurance Plan. In turn, these plans must include strict controls on the procurement of materials and services. Those controls ensure "that applicable regulatory requirements, design bases, and other requirements which are necessary to assure adequate quality are suitably included or referenced in the documents for procurement of material, equipment, and services, whether purchased by the applicant or by its contractors or subcontractors."[10] To

---

program to protect those digital computer and communication systems and networks identified in 10 CFR 73.54(a)(1) into the site physical protection program requires that the high assurance of adequate protection standard for physical protection be applied to the protection of these systems.

6 10 CFR 73.54(a)(2).

7 The NRC conducts inspections to ensure that operating power reactor licensees are implementing the cybersecurity programs at their facilities as described in their NRC-accepted cybersecurity plans. *See*, *e.g.*, NRC Inspection Procedure 71130.10P, "Cyber Security."

8 For example, NRC Regulatory Guide (RG) 5.71, "Cyber Security Programs for Nuclear Facilities," (January 2010), provides a comprehensive approach to comply with 10 CFR 73.54 for cybersecurity by using strategies in NIST SP 800-53, Revision 4, "Recommended Security Controls for Federal Information Systems." RG 5.71 is currently undergoing revision by the NRC. See Draft Regulatory Guide (DG)-5061, "Cyber Security Programs for Nuclear Power Reactors," (August 2018). NEI has issued NEI-08-09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors," (April 2010) to further support industry compliance with the relevant NRC requirements.

9 Specifically, RG 5.71 directs licensees to protect against supply chain threats and vulnerability by employing the following measures to protect against supply chain threats to maintain the integrity of acquired critical digital assets: (1) establishing trusted distribution paths, (2) validating vendors, and (3) requiring tamper-proof products or tamper-evident seals on acquired products. Licensees are further directed to perform an analysis for each product acquisition to determine that the product provides the security requirements necessary to address the security controls in Appendices B and C to RG 5.71, and to use heterogeneity to mitigate vulnerabilities associated with the use of a single vendor's product.

10 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," at Criteria IV, "Procurement Document Control."

the extent necessary, these procurement documents must also require contractors or subcontractors to provide a quality assurance program consistent with Appendix B.[11]

Further, licensees subject to Appendix B must ensure that purchased material, equipment, and services purchased from vendors – whether directly or through contractors and subcontractors – conform to the procurement documents.[12] This assurance is achieved through source evaluation and selection, objective evidence of quality furnished by the contractor or subcontractor, inspection at the contractor or subcontractor source, and examination of products upon delivery. Before installing or using material or equipment subject to the quality assurance requirements, licensees must establish (and maintain) documentary evidence that such material and equipment conform to the procurement requirements. This documentary evidence, which also is subject to NRC inspection, must be sufficient to identify the specific requirements (*e.g.*, codes, standards, or specifications) met by the purchased material and equipment.[13] Finally, the licensee is required to assess the effectiveness of the control of quality by contractors and subcontractors at intervals consistent with the importance, complexity, and quantity of the product or services.

In a related vein, NRC regulations in 10 CFR Part 21 establish requirements for the reporting of defects and noncompliances by entities and persons owning, operating or supplying basic components for any facility or activity licensed or otherwise regulated pursuant to the Atomic Energy Act of 1954, as amended. Among other things, the NRC conducts vendor inspections of suppliers of safety-related critical digital assets, and evaluates the results of these inspections to determine the need to expand the inspection sample to suppliers and sub-suppliers of non-safety-related critical digital assets. Additionally, power reactors licensees oversee their vendors in accordance with the licensees' NRC-approved Quality Assurance Plans. These oversight activities include periodic vendor audits, oversight of critical construction activities, receipt inspections, use of a corrective action program (CAP) to identify and correct errors as well as annual reviews of vendor performance. Thus, both the NRC requirements directly applicable to vendors, as well as the inspections and audits conducted by the NRC and licensees, respectively, help to address supply chain cyber security risks.

We believe that the NRC's cybersecurity and quality assurance requirements, and the programs developed by the nation's nuclear power fleet to comply with those requirements, currently address the major concerns that prompted issuance of EO 13990 insofar as they apply to commercial nuclear power plants. It is well understood that protecting nuclear generating assets provides reliability and security to the BPS.

Given the already-robust regulatory framework described above, we do not see the need for any additional assistance, security requirements, or procurement practices to be imposed on the commercial nuclear power

---

11 *Id.*

12 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," at Criteria VII "Control of Purchased Material, Equipment, and Services."

13 *See* NRC Inspection Procedure (IP) 43002, "Routine Inspections of Nuclear Vendors," (Jan. 2017).

fleet at this time.[14] Further, we do not see a need to issue any prohibition order(s) on equipment or infrastructure associated with the commercial nuclear power fleet.[15]

Therefore, we respectfully request that DOE avoid imposing additional, redundant requirements on nuclear power facilities. Insofar as DOE might wish to further consider whether the current requirements applicable to commercial nuclear power plants are sufficient to prevent exploitation and attacks by foreign threats to the U.S. supply chain, it should coordinate such efforts with the NRC and NERC. If DOE believes that additional requirements or measures are warranted in the area of nuclear power plant cybersecurity, then DOE should engage NERC and NRC to determine how such requirements or measures should be developed and implemented. For example, if any modifications to the current NRC-NERC MOU were to prove necessary, then NEI requests that DOE work closely with the NRC and NERC to maintain the clarity currently provided by the document, including clearly defining the scope of oversight to be provided by NRC, NERC, and DOE.

If you have any questions, please contact me or Pete Kissinger at pwk@nei.org or (612) 419-3602.

Sincerely,

Jennifer L. Uhle

---

[14] *See* 86 Fed. Reg. 21310-11 (questions 1 through 4 related to long-term strategy).

[15] *See Id.* at 21311 (questions 1 through 4 related to prohibition authority).