Talking Points: NEI Approach to Revising Cyber Security Guidance for Balance of Plant Digital Assets:

Key Message:

- The Nuclear Energy Institute (NEI) has prepared a white paper for the U.S. Nuclear Regulatory Commission (NRC) approval that proposes changes to NEI guidance for identifying and protecting Balance of Plant (BOP) Critical Digital Assets (CDAs). The changes are intended to improve the efficiency of licensee cyber security programs while maintaining program effectiveness to protect against cyber attacks. The proposed changes will be incorporated into a future revision to NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012, and NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017. These changes are intended to ensure NRC licensees are protecting BOP assets at a level commensurate with the plant's risk to the reliability of the Bulk Electric System (BES) associated with non-nuclear generators.

History of NRC and Federal Energy Regulatory Commission (FERC):

- In January 2008, FERC issued Order No. 706, which specified Critical Infrastructure Protection (CIP) Reliability Standards to safeguard critical cyber assets. The requirements in Order No. 706 applied to certain users, owners, and operators of the bulk-power system. Order No. 706 specifically exempted "facilities regulated by the NRC" from these requirements.

- In March of 2009, the NRC issued Title 10 of the *Code of Federal Regulations* (10 CFR)73.54," Protection of Digital Computer, Communication, and Networks" to NRC power reactor licensees. This regulation did not cover all balance-of-plant equipment at NRC power reactor facilities and it was later determined that this exemption created a potential gap between the NRC and FERC cyber security requirements. The scope of systems under 10 CFR 73.54 includes systems associated with safety, important-to-safety, security, and emergency preparedness (SSEP) functions, as well as support systems and equipment that if compromised could adversely impact SSEP functions.

- The NRC staff did not consider many of the BOP structures systems and components (SSCs) to be within the scope of 10 CFR 73.54. Therefore, the staff believed that these BOP SSCs fell within the scope of North American Electric Reliability Corporations (NERC's) CIP standards.

- On March 19, 2009, FERC issued Order No. 706-B to address this potential gap by clarifying that the BOP systems and equipment within a Nuclear Power Plant (NPP) that are not within the scope of 10 CFR 73.54 are subject to compliance with the CIP standards approved in Order No. 706. The order allowed nuclear facilities to seek exceptions from NERC's CIP standards on a case-by-case basis for those digital assets subject to the NRC's cyber security requirements.

- In October 2009, the NRC staff briefed the Commission on NRC and NERC cyber security jurisdictional issues, future cyber security inspections at NRC-licensed NPPs, and the status of the memorandum of understanding (MOU) between the NRC and NERC.

- In December 2009, the NRC and NERC entered into an MOU addressing how NRC and NERC would cooperate on handling their respective authority over cyber security issues at NPPs. The NRC and NERC committed to cooperate in considering specific exception requests from NPPs in the December 2009 MOU. This MOU was renewed in December of 2015.

- In 2009, the NRC and FERC entered a Memorandum of Agreement to facilitate a continuing and cooperative relationship between the two regulatory agencies on matters of mutual interest related to the nation's electric power grid reliability and nuclear power plant safety and security, including coordination of activities related to cybersecurity.

- NERC subsequently sent a letter to all NPPs, known as the “Bright-Line” survey, requesting that, by June 24, 2010, all NPPs determine which of their SSCs were potentially subject to NERC CIP standards and which were potentially subject to NRC cyber security regulations. All NRC NPP licensees declared in their responses that the BOP SSCs, if compromised, affect reactivity and are important-to-safety. NRC NPP licensees further stated that for this reason, all BOP SSCs fall within the scope of the NRC’s cyber security regulations.

- In a letter dated August 9, 2010, NERC informed the NRC that based on the responses to the Bright-Line Survey, NERC has determined that the assignment of regulatory authority for the BOP SSCs from the NERC CIP standards to the NRC cyber security authority is conditionally acceptable. The conditions specified by NERC are that licensees notify the NRC by letter of all BOP SSCs licensees consider important-to-safety and submit a revised cyber security plan (CSP) to the NRC for review and approval. In late August 2010, NERC sent a letter to all NRC NPP licensees stating these requirements. Each licensee sent the requested notification letter to the NRC and committed to update their CSP to include BOP SSCs within their plans.

- On October 21, 2010, the NRC Commission determined as a matter of policy that the NRC’s cyber security rule at 10 CFR § 73.54 should be interpreted to include SSCs in the BOP that have a nexus to radiological health and safety at NRC-licensed NPPs. The NRC has statutory authority to assume this responsibility and the Commission has concluded that doing so would enhance nuclear safety and regulatory efficiency.

- In November 2012, NERC adopted CIP-002-5 which revised how to identify and categorize BES Cyber Systems and their associated cyber sssets based on the adverse impact that loss, compromise, or misuse of those BES cyber systems could have on the reliable operation of the BES. The impact rating criteria divides cyber systems into High, Medium, and Low Impact Ratings to provide a graded approach to applying cyber security controls based upon risk-based impact to the BES. This approach has remained consistent through the current revision, CIP-002-5.1a.