NRC Staff Comments on NEI 15-09, "Cyber Security Event Notifications," Revision 1, Dated May 2022

NEI 15-09 Location	NEI 15-09 Text	Revised Text for Consideration	NRC Staff Comment and Technical Basis
Section 1.4, "Related Guidance"	"U.S. Department of Homeland Security's website provides a vast amount of information related to cyber security and cyber security event reporting (www.dhs.gov)."	N/A	Recommend including a link to DHS/CISA's website for reporting cyber events, https://www.cisa.gov/report.
Executive Summary	Summary of Changes	N/A	The summary of changes should address changes made to Section 2.1.1 regarding 1-hour reportable events.
Section 2.1.1	"Therefore, it is the CDAs identified by the licensee's Cyber Security Plan that are subject to the reporting requirements in 10 CFR 73.77…"	"Therefore, it is the CDAs identified by the licensee's Cyber Security Plan that are subject to the reporting requirements in 10 CFR 73.77(a)(1)…"	This statement should specify that it pertains to 1-hour reports under 10 CFR 73.77(a)(1). Malicious activity against non-CDA devices that provide protection to CDAs or perform support functions are reportable under 10 CFR 73.77(a)(3).
Appendix C	Eight-hour Notifications		Malicious cyber actors routinely target devices that provide real-time detection and alerting as part of their pre-operational activities against critical targets. Actions by malicious cyber actors against devices from which a CDA inherits

			security controls (e.g., portable media scanning kiosks, intrusion detection/prevention systems, security information and event management systems) are examples of such activity. This activity is reportable under 10 CFR 73.77(a)(3) as, “observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer and communication systems and networks within the scope of 10 CFR 73.54.” NEI 15-09 should provide guidance and examples to this effect.
Appendix C	Eight-hour Notifications		Malicious cyber activity observed against or impacting non-CDA digital systems located on the same network as a CDA would indicate potential pre-operational activity that could affect CDAs.

			This activity is reportable under 10 CFR 73.77(a)(3) as, “observed behavior, activities, or statements that may indicate intelligence gathering or pre-operational planning related to a cyber attack against digital computer and communication systems and networks within the scope of 10 CFR 73.54.” NEI 15-09 should provide guidance and examples to this effect.