Proposed Resolution – Glossary and Reporting

Glossary Resolution Table

The proposed revisions to NEI 08-09, Revision 3, Appendix B, "Glossary" are provided below. All other glossary terms have been deleted. The table below contains three columns, as labeled. In the final NEI 08-09, Revsion 6, only the right-hand column resolution will be implemented. Also, the following text will be added to the beginning of Appendix B as a Guide to users to provide references to other documents for the resolution of terms not defined in NEI 08-09:

> The glossary in NEI 08-09 defines only those terms that are specific to their usage in NEI 08-09. Other terms should be referenced in the following order of preference.
>
> 1. Specific terms defined in Rules.
> 2. NEI Scope of Systems white paper for clarification of 73.54(a)(1) systems.
> 3. NIST IR 7298 Glossary of Key Information Security Terms.
> 4. RG 5.71 Rev. 0, January 2010
> 5. Webster's dictionary

Current NEI 08-09 Definition	**Current RG 5.71 Definition**	**Proposed Resolution, New Definition**
Adversary An individual who does not possess authorized unescorted access to the Protected Area and that is actively engaged in an attempted unauthorized entry of the Protected or Vidal Areas for the purpose of attempting an act of radiological sabotage.	**Adversary** Individual, group, or organization that conducts or has the intent to conduct detrimental activities. (DHS Source)	Revise NEI 08-09 Rev 3 Appendix B to read as follows: Revise the definition of "Adversary" to: Individual, group, or organization that is conducting or is attempting to conduct a cyber attack.
Critical Digital Asset (CDA) A digital device or system that plays a role in the operation or maintenance of a critical system and can impact the proper functioning of that critical system. A CDA may be a component or a subsystem of a critical system; the CDA may by itself be a critical system; or the CDA may have a direct or indirect connection to a critical system. Direct connections include both wired and wireless communication pathways.	**Critical Digital Asset (CDA)** A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network.	Revise the definition in Appendix B to read as follows: Revise the definition of "Critical Digital Asset" to: A digital computer, communication system, or network whose failure or compromise as the result of a cyber attack would result in the failure or degradation of an SSEP function. [Note: This definition is derived from 73.54(a)]

Current NEI 08-09 Definition	Current RG 5.71 Definition	Proposed Resolution, New Definition
Indirect connections include pathways by which data or software are manually carried from one digital device to another and transferred using disks or other modes of data transfer. (Source: NUREG 6847/NEI 04-04 R1)		
Critical System (CS) A system in a plant that can adversely impact the safety, important-to safety, security, and emergency preparedness functions of a nuclear power plant. These systems include safety systems, plant security, operational control systems, emergency preparedness, and auxiliary systems that support safety systems.	**Critical System (CS)** An analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment, that perform or are associated with a safety-related, important-to-safety, security, or emergency preparedness function.	Revise NEI 08-09 Rev 3 Appendix B to read as follows: Revise the definition of "Critical System" to: A system that provides safety-related functions; important-to-safety functions; security functions; emergency preparedness functions, including offsite communications; or support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions. [Note: Revise NEI 08-09, Revision 3, Appendix A, Section 3.1.3 to reference the definition above.]
Cyber Attack Any event in which there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause the willful, malicious exploitation of site computer and communication systems to modify or destroy data, modify or destroy programming code or executables, deny access to	**Cyber Attack** The manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may (1) originate from either inside or outside the licensee's facility, (2) have internal and external components, (3) involve	Revise NEI 08-09 Rev 3 Appendix B to read as follows: Revise the definition of "Cyber Attack" to: Any event where there is reason to believe that an adversary has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause the interruption of safe nuclear plant operation through, malicious

Current NEI 08-09 Definition	Current RG 5.71 Definition	Proposed Resolution, New Definition
systems, or prevent the intended operation of a CDA. (Source: This Document)	physical or logical threats, (4) be directed or non directed in nature, (5) be conducted by threat agents having either malicious or non malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to critical digital assets or critical systems. This includes attempts to gain unauthorized access to a CDA and/or CS's services, resources, or information, the attempt to compromise a CDA and/or CSs integrity, availability, or confidentiality or the attempt to cause an adverse impact to a SSEP function. Further background on cyber attacks which are up to and including DBT, can be found in Sections 1.1(c), 1.2, and 1.5 of Regulatory Guide 5.69, and the cyber attack may occur individually or in any combination.	exploitation of a CDA. [Note: Derived from the following sources: 10CFR73.71(b); 10CFR73 Appendix G; DG-5019, 10CFR 73.55(f); 72 FR 12723, 12724]
Cyber Incident A non-malicious and/or inadvertent act associated with the failure or degradation of a critical digital asset that causes a condition defined as "adverse" in the Corrective Action Program. (Source: This Document)	**Cyber Incident** SEE INCIDENT **Incident** Occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action.	Revise NEI 08-09 Rev 3 Appendix B to read as follows: Revise to delete the definition of Cyber Incident. Revise NEI 08-09, Revision 3 to replace "Incident" with "Attack" where appropriate.

The proposed revision to NEI 08-09, Revision 3, Appendix C, "Reporting Cyber Attacks" is provided below. The entirety of Appendix C will be replaced with the text below.

APPENDIX C

REPORTING CYBER ATTACKS

Part 73, Appendix G, paragraph I.(a)(3) requires specific events to be reported within one (1) hour of discovery, followed by a written report within 60 days. The following criteria may be used to help establish Cyber Attack reporting procedures:

Reporting Criteria	Decision Logic
Part 73, Appendix G, paragraph I.(a)(3): "Any event in which there is reason to believe that a person has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause interruption of normal operation of a licensed nuclear power reactor through the unauthorized use of or tampering with its machinery, components, or controls including the security system."	1. Is the SSC classified as a CDA in the Site Cyber Security Program? 2. Is there "reason to believe" that an adversary has attempted a Cyber Attack? The following example criteria may be used to help establish "reason to believe." a. Evidence of targeted, malicious attempts to scan or probe a CDA; b. Evidence of unauthorized attempts to gain access to or tamper with a CDA; or c. Evidence of unauthorized executable code residing on or communicating with a CDA. 3. Establishing "Reason to believe" determines the time of discovery for the one (1) hour and sixty (60) day reports.

.