NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
October 29, 2018, Informal Posting

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
Cyber Asset (CA)	Programmable electronic devices, including the hardware, software, and data in those devices.	A p~~P~~rogrammable electronic device~~s~~, including the physical or virtual hardware, software, and data in th~~os~~e device~~s~~.
BES Cyber System (BCS)	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.	Any combination of hardware (including virtual hardware), software (including application virtualization), and data, regardless of redundancy, performing one or more reliability tasks that if rendered unavailable, degraded, or misused would result in adverse impact to one or more BES Facilities within 15 minutes.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
BES Cyber Asset (BCA)	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse	Retired

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber Asset, • network within an Electronic Security Perimeter (ESP) containing high or medium impact BES Cyber Systems, or • PCA associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.	A Cyber Asset that is: 1. capable of transmitting or transferring executable code, 2. not included in a BES Cyber System, 3. not a Protected Cyber ~~Asset~~ System (PC~~S~~A) associated with high or medium impact BES Cyber Systems, and 4. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a: • BES Cyber ~~Asset~~System (BCS), • ~~network within an~~ A BES Cyber System Logical Isolation Zone ~~Electronic Security Perimeter (ESP)~~ containing high or medium impact BES Cyber Systems, or • PC~~S~~A associated with high or medium impact BES Cyber Systems. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Physical Access Control Systems (PACS)	Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.	Cyber systems ~~Assets~~ that control~~, alert, or log~~ access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Physical Access Monitoring Systems (PAMS)	N/A	Cyber systems that alert or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.
Protected Cyber Asset (PCA)	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.	Retired
Protected Cyber System (PCS)	N/A	Cyber systems that are able to communicate with a BES Cyber System from within the BES Cyber System's Logical Isolation Zone. The impact rating of Protected Cyber Systems is equal to the highest rated BES Cyber System within the Logical Isolation Zone.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Electronic Access Point (EAP)	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.	Retired
Electronic Access Control or Monitoring Systems (EACMS)	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.	RETIRED – Proposed Develop EAMS and EACS
Electronic Access Control System (EACS)	N/A	Cyber systems that provide electronic access control to BES Cyber Systems.
Electronic Access Monitoring Systems (EAMS)	N/A	Cyber systems that provide electronic access monitoring of BES Cyber Systems.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	Retired
External Routable Connectivity (ERC)	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Logical Isolation Zone via a bi-directional routable protocol connection.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Logical Isolation Zone (LIZ)	N/A	A logical security zone created by applying controls to communications to or from BES Cyber Systems and Protected Cyber Systems.
Intermediate Systems (IS)	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	A system acting as part of the protection applied to a logically isolated BCS that limits external user-initiated access to authorized users.
Interactive Remote Access (IRA)	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.	User-initiated access by a person employing a remote access client to a BES Cyber System or Protected Cyber System from outside of a Logical Isolation Zone. Interactive Remote Access does not include system-to-system process communications or access initiated from an Intermediate System.

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Physical Security Perimeter (PSP)	The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.	The physical border surrounding locations in which~~,~~ ~~BES Cyber Assets,~~ BES Cyber Systems~~,~~ or Electronic Access Control ~~or Monitoring~~ Systems reside~~,~~ and for which access is controlled.
Removable Media	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.	Storage media that (i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber ~~Asset~~System, ~~a network within an ESP,~~ or a Protected Cyber ~~Asset~~System. ~~Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.~~
Secure Configuration	N/A	The implemented set of controls supporting the security objectives found within the CIP Reliability Standards where the following text exists within the requirement language: "NOTE: The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system."