CIP Definitions

Project 2016-02 Modifications to CIP Standards

This SDT is seeking comment on the following new, modified, or retired terms used in the proposed standard. Please note that Project 2016-02 is not proposing changes to Cyber Asset (CA), BES Cyber System (BCS), or Electronic Security Perimeter (ESP) definitions to maintain compatibility for non-virtualized systems.

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 impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.	A Cyber Asset or Virtual Cyber Asset; excluding Shared Cyber Infrastructure, 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 impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
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.	Cyber Assets or Virtual Cyber Assets that perform electronic access control or electronic access monitoring or the logical isolation of BES Cyber Systems. This includes Intermediate Systems.

DRAFT

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 with a comment inserted in the NERC Glossary inactive date.
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 or Virtual Cyber Asset through a system controlling communications to and from the BES Cyber System via a bi-directional routable protocol connection.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	

DRAFT

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
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.
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 type of EACMS that is used to restrict Interactive Remote Access.
Management Interface		A physical or logical interface of a Cyber Asset or SCI that provides management and monitoring capabilities.
Management Module		An autonomous subsystem of a Cyber Asset or SCI that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI), and operating system.

DRAFT

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Management Systems		Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Virtual Cyber Assets or Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.
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 at which access is controlled.
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.	Cyber Assets or Virtual Cyber Assets that: • Are not logically isolated from a BES Cyber System; or • Share compute resources (CPU or memory) with a BES Cyber System, excluding logically isolated cyber assets or virtual cyber assets that are being actively remediated prior to introduction to the production environment.

DRAFT

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
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, a Protected Cyber Asset, SCI or a network that is not logically isolated from high or medium impact BES Cyber Systems.
Self-Contained Application		Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.
Shared Cyber Infrastructure (SCI)		One or more programmable electronic devices (excluding Management Modules) and their software that share their computer or storage resources with one or more Virtual Cyber Assets or other Cyber Assets; including Management Systems used to initialize, deploy, or configure the SCI.

DRAFT

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 or Virtual 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, • Shared Cyber Infrastructure, • PCA associated with high or medium impact BES Cyber Systems, or • Network that is not logically isolated from 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.

DRAFT

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
Virtual Cyber Asset (VCA)		A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure.

DRAFT