NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards

The standard drafting team (SDT) is seeking comment on the following new, modified, or retired terms used in the proposed standards. The first column (*NERC Glossary Term*) provides the NERC Glossary term being modified or proposed as a new. The SDT is proposing acronyms to some currently approved and new glossary terms as shown in redline. The second column (*Currently Approved Definition*) provides the currently approved definition and the third column (*CIP SDT Proposed New or Revised)* reflects the proposed modifications to the current definitions in redline and also reflects newly proposed definitions in clean view.

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, 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.
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.	One or more BES Cyber Assets logically grouped by a R~~r~~esponsible E~~e~~ntity to perform one or more reliability tasks for a functional entity, including Shared Cyber Infrastructure grouped, by the Responsible Entity, in the BES Cyber System it supports.
BES Cyber System Information	Information about the BES Cyber System that could be used to gain	Information about the BES Cyber System or Shared Cyber

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
(BCSI)	unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System	Infrastructure that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. BES Cyber System Information does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BES Cyber System
CIP Senior Manager	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.	A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC Critical Infrastructure Protection Standards~~,~~ ~~CIP-002 through CIP-011.~~
CIP System *New Definition*		A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.
Cyber Security Incident	A malicious act or suspicious event that: - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or - Disrupts or attempts to disrupt the operation of a BES Cyber System	A malicious act or suspicious event that: • ~~–~~For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or (4) Shared Cyber Infrastructure; or • Disrupts or attempts to disrupt the operation of a BES Cyber System.
Cyber System ***New Definition***		A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.
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, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems or SCI. This includes Intermediate Systems and SCI grouped, by the Responsible Entity, in the EACMS it supports.
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	A policy enforcement point or a Cyber Asset interface~~on an Electronic Security Perimeter~~ that allows routable communication ~~between Cyber Assets outside an~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	Cyber Assets inside an Electronic Security Perimeter.	~~Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter~~to and from the BES Cyber System within an Electronic Security Perimeter.
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 communicate to a CIP System using ~~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~~from outside the asset containing the CIP System.
Electronic Security Perimeter (ESP)	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.	~~The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.~~ A set of configurations or policies enforced by an EACMS that controls communications to or from any part of a BES Cyber System. These configurations or policies group CIP Systems of the same impact rating and their associated PCAs.
~~**Cyber System**~~		~~A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.~~
~~**CIP System**~~		~~A Cyber System identified by the Responsible Entity as a BES Cyber System, Electronic Access Control or Monitoring System, Physical Access Control System, Shared Cyber Infrastructure, Protected Cyber Asset, or Transient Cyber Asset.~~
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	User-initiated real-time access by a person from outside of the Responsible Entity's Electronic Security Perimeters (ESP)~~.~~ using a

Table 1: Retired, Modified, or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised**
	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.	routable protocol: • to a Cyber System within an ESP; • through a Cyber Asset or Virtual Cyber Asset that is converting communications from a routable protocol to a non-routable protocol to a Cyber System not within an Electronic Security Perimeter; • To Management Interfaces of ~~an~~ Shared Cyber Infrastructure; or • To Management Interfaces of an Electronic Access Control or Monitoring Systems that enforces an ESP. ~~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.~~
Intermediate Systems	A Cyber Asset or collection of Cyber Assets performing access control to	One or more Electronic Access Control or Monitoring Systems that

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.	~~is~~are used to restrict Interactive Remote Access to only authorized users.~~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.~~
Management Interface ***New Definition***		A user interface, logical interface, or dedicated physical port that is used to: • Control the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; or • Provide lights-out management capabilities; or • Configure an Electronic Security Perimeter; excluding physical user interfaces (e.g., power switch, touch panel, etc.).
~~**Management Module**~~		~~An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.~~
~~**Management Systems**~~		~~Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		~~those assets and systems; excluding Management Modules.~~
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 Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) (including SCI grouped, by the Responsible Entity, in the Physical Access Control Systems it supports) 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 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, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for 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.	One or more Cyber Assets or Virtual Cyber Assets that: • Are within an Electronic Security Perimeter but are not part of the highest impact BES Cyber System within the same Electronic Security Perimeter; or • Share CPU or memory with any part of a BES Cyber System, excluding Virtual Cyber Assets that are being actively remediated prior to introduction to the Electronic Security Perimeter. ~~connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		~~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.~~
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 or Shared Cyber Infrastructure, (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, Shared Cyber Infrastructure, 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.~~
Reportable Cyber Security Incident	A Cyber Security Incident that compromised or disrupted: - A BES Cyber System that performs one or more reliability tasks of a functional entity; - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	A Cyber Security Incident that compromised or disrupted: • ~~-~~A BES Cyber System that performs one or more reliability tasks of a functional entity; • ~~-~~An Electronic Security Perimeter of a high or medium impact BES Cyber System; ~~or~~ • ~~-~~An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or • -Shared Cyber Infrastructure supporting a BES Cyber System
~~**Self-Contained Application**~~		~~Immutable software binaries containing operating system~~

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		~~dependencies and application software packaged to execute in an isolated environment.~~
Shared Cyber Infrastructure (SCI) ***New Definition***	One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.	One or more programmable electronic devices, including the software and Management Interfaces, that share: • CPU and memory resources with one or more Virtual Cyber Assets identified as a BCA, EACMS, or PACS; or • storage resources with any part of a BES Cyber System or their associated ~~Electronic Access Control or Monitoring Systems~~EACMS or ~~Physical Access Control Systems~~PACS. Each SCI is either: • included in one or more BES Cyber Systems, EACMS, or PACS; or • identified independently. SCI does not include the supported VCA or CA with which it shares its resources. ~~(excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.~~
Transient Cyber Asset (TCA)	A Cyber Asset that is: 1. capable of transmitting or transferring executable code,	A Cyber Asset or Virtual Cyber Asset that is: 1. capable of transmitting or

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
	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.	transferring executable code, 2. not included in a BES Cyber System, ~~2. not a Shared Cyber Infrastructure associated with high or medium impact BES Cyber Systems~~ 3. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and 4. connected for 30 consecutive calendar days or less: • to a network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or • 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, or ▪ ~~Network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or~~ Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Table 1: Retired, Modified, or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised
		Virtual machines hosted on a physical TCA can be treated as software on that physical TCA. Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.
Virtual Cyber Asset (VCA) ***New Definition***		A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a PCA.