NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Definitions

Project 2016-02 Modifications to CIP Standards
Draft 5

The standard drafting team (SDT) is seeking comment on the following new or modified 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: Modified or Newly Proposed Definitions

NERC Glossary Term	Currently Approved Definition	CIP SDT Proposed New or Revised REDLINE TO Currently Approved
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~~Reliable Operation of the Bulk Electric System~~.~~ (BES). 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	

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
Update is Acronym only.	by a responsible entity to perform one or more reliability tasks for a functional entity.	
BES Cyber System Information (BCSI)	Information about the BES Cyber System 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, 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	Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the ~~BES Cyber System~~BCS. BES Cyber System Information (BCSI) 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~~BCS, such as, but not limited to, device names, individual IP addresses without context, ~~ESP~~Electronic Security Perimeter names, or policy statements. Examples of ~~BES Cyber System Information~~BCSI may include, but are not limited to, security procedures or security information about ~~BES~~BCS, Shared Cyber ~~Systems~~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~~BCS.
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	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

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	CIP Standards, CIP-002 through CIP-011.	~~CIP~~Critical Infrastructure Protection Cyber Security Standards~~, CIP-002 through CIP-011.~~.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.	Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCAs) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.
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~~,~~ (BCS), 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~~BCS.
Cyber System ***New Definition***		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	Cyber ~~Assets~~System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	Systems. This includes Intermediate Systems.	Systems (BCS). ~~This includes Intermediate Systems.~~, including those not protected by an Electronic Security Perimeter used by the responsible entity to convert routable protocol communications to non-routable communications to a BCS.
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.	~~A~~An electronic policy enforcement point or a Cyber Asset interface on an Electronic ~~Security Perimeter~~Access Control or Monitoring Systems that ~~allows~~controls routable communication ~~between~~to and from one or more BES Cyber Systems or their associated Protected Cyber Assets ~~outside an Electronic Security Perimeter and Cyber Assets inside 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 access a BES Cyber System ~~from a Cyber Asset that is outside of its associated~~through its Electronic Security Perimeter 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.	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.
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	User-initiated electronic access by a person ~~employing a remote access client or other remote access technology~~ using a bi-directional routable protocol ~~. Remote access originates from a Cyber Asset that is not an Intermediate~~ :

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	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.	• To a Cyber System ~~and not located within any of the Responsible Entity's~~ protected by an Electronic Security Perimeter(s) ~~or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) (ESP);~~ • That is converted by the responsible entity to a non-routable protocol that allows access to a 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.~~ System; or • To a Management Interface. Interactive ~~r~~Remote ~~a~~Access does not include ~~system~~: • Communication that originates from a Cyber System protected by any of the Responsible Entity's ESPs; or System-to-system process communication~~s~~.
Intermediate System	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 Cyber Asset~~One or ~~collection of Cyber Assets performing access control~~more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users. ~~The Intermediate System must not be located inside the Electronic Security Perimeter.~~

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
Management Interface *New Definition*		An administrative interface that: • Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure; • Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or • Configures an Electronic Access Point.
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~~Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the ~~Physical Security Perimeter~~PSP 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 ~~connected using a routable protocol within~~ or ~~on~~Virtual Cyber Assets that: • Are protected by an Electronic Security Perimeter ~~that is~~(ESP) but are not part of the highest impact BES Cyber System ~~within~~(BCS) protected by the same ~~Electronic Security Perimeter. The impact~~

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		~~rating~~ESP; or • Share CPU resources or memory resources with any part of ~~Protected Cyber Assets is equal to~~ the ~~highest rated BES~~BCS, excluding Virtual Cyber ~~System~~Assets that are being actively remediated in ~~the same ESP.~~an environment that isolates routable connectivity from BCS; Excluding Transient Cyber Assets.
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 (SCI), (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, SCI, a network ~~within~~protected by an ~~ESP~~Electronic Security Perimeter, 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	A Cyber Security Incident that compromised or disrupted: • ~~–~~A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity; • ~~–~~An Electronic Security Perimeter of a high

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System	or medium impact ~~BES Cyber System; or~~BCS; • ~~-~~An Electronic Access Control or Monitoring Systems of a high or medium impact ~~BES~~BCS; or • Shared Cyber ~~System~~Infrastructure supporting a BCS.
Shared Cyber Infrastructure (SCI) ***New Definition***		One or more programmable electronic devices, including the software that shares the devices' resources, that: • Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber Systems (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or • Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization. SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.
Transient Cyber Asset (TCA)	A Cyber Asset that is:	A Cyber Asset or Virtual Cyber Asset (VCA) that is:

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
	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.	1. ~~c~~Capable of transmitting or transferring executable code, 2. ~~n~~Not included in a BES Cyber System (BCS), 3. ~~n~~Not a Protected Cyber Asset (PCA) associated with high or medium impact ~~BES Cyber Systems~~BCS, and 4. ~~directly c~~Connected for 30 consecutive calendar days or less: • On a network protected by an Electronic Security Perimeter (ESP) containing high or medium impact BCS, or • Directly (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:~~to a: ~~•~~ BES Cyber Asset, ▪ ~~network within an Electronic Security Perimeter (ESP) containing high~~ or ~~medium impact BES Cyber Systems, or~~ ▪ Shared Cyber Infrastructure, or ▪ PCA associated with high or medium impact ~~BES Cyber Systems~~BCS.

Table 1: Modified or Newly Proposed Definitions		
NERC Glossary Term	**Currently Approved Definition**	**CIP SDT Proposed New or Revised REDLINE TO Currently Approved**
		~~Examples of~~ Virtual machines hosted on a physical Transient Cyber Asset~~s~~ (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs 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, currently executing on a virtual machine hosted on a BES Cyber Asset; Electronic Access Control or Monitoring System; Physical Access Control System; Protected Cyber Asset; or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include: • Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems; • Dormant file-based images that contain operating systems or firmware; and • SCI or Cyber Assets that host VCAs. Application containers are considered software of VCAs or Cyber Assets.