Definitions of Terms Used in Version 5 CIP Cyber Security Standards

This section includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards and proposes terms for retirement. Terms already defined in the Glossary of Terms used in NERC Reliability Standards are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary. New defined terms are underscored. For existing glossary terms, new language is shown as underscored, while deleted language is shown as stricken. The list of terms proposed for retirement is at the end of the document.

Note: On September 21, 2012, consistent with corrections to CIP-002-5, this draft was revised to correct the incorrect functional model reference in Control Center from "Generation Operator" to "Generator Operator"

No other changes were made to the definitions or any of the other CIP V5 standards currently posted, except as specified in CIP-002-5.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, ~~Systems~~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~~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 is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

~~**Cyber Security Incident**~~

~~Any A malicious act or suspicious event that:~~

- ~~Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,~~
- ~~Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset BES Cyber System.~~

[SWN1]

BES Cyber System

One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.

BES Cyber System Information

Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. ~~Examples of BES Cyber System Information may include, but are not limited to, security procedures developed by the responsible entity and security information about BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of 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.

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death, a natural disaster, civil unrest, an imminent or existing hardware, software, or equipment failure, a Cyber Security Incident requiring emergency assistance, a response by emergency services, the enactment of a mutual assistance agreement, or an impediment of large scale workforce availability.

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.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability ~~functional~~ tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for ~~Transmission~~transmission Facilities at two or more locations, or 4) a ~~Generation~~ Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, ~~and communication networks~~ including the hardware, software, and data in those devices.

Cyber Security Incident

~~Any~~ A malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter ~~of a Critical Cyber Asset~~, or~~,~~
- Disrupts, or was an attempt to disrupt, the operation of a ~~Critical Cyber Asset~~ BES Cyber System.

Dial-up Connectivity

A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

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 Devices.

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.

Electronic Security Perimeter ("ESP")

The logical border surrounding a network to which ~~Critical Cyber Assets~~ BES Cyber Systems are connected using a routable protocol ~~and for which access is controlled~~.

External Routable Connectivity

~~A~~ The ability to access a BES Cyber System ~~that is accessible~~ from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.

Interactive Remote Access

~~All user~~User-initiated access by a person ~~that~~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 Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s~~), whether routable~~) or ~~dial-up access, using~~at a ~~client or remote access technology.~~ 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 Device

A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate Device must not be located inside the Electronic Security Perimeter.

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.

Physical Security Perimeter ("PSP")

~~The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.~~

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled.

Protected Cyber ~~Asset~~Assets ("PCA")

~~A~~One or more Cyber ~~Asset~~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 ~~(a~~. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP. A Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is ~~directly~~ connected either to a Cyber Asset within ~~an~~the ESP or to ~~a BES Cyber Asset~~the network within the ESP, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes~~).~~.

Reportable Cyber Security Incident

~~Any~~A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.

Terms to be retired from the *Glossary of Terms used in NERC Reliability Standards* once the standards that use those terms are replaced:

Critical Assets

Critical Cyber Assets