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.

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

BES Cyber Asset

A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its operation, mis-operation, or non-operation, when required, adversely impact one or more BES Reliability Operating Services. This is regardless of the delay between the point in time of unavailability, degradation, or misuse of the Cyber Asset and the point in time of impact on the BES Reliability Operating Services. The timeframe is not in respect to any cyber security events or incidents, but is related to the time between when the Cyber Asset can send or receive instructions to operate and the time in which that operation occurs and impacts the BES. Redundancy shall not be considered when determining availability. A Transient Cyber Asset is not considered a BES Cyber Asset.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

BES 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, or
- Results in unauthorized physical access into a Defined Physical Boundary .

BES Cyber System

One or more BES Cyber Assets that are typically grouped together, logically or physically, to operate one or more BES Reliability Operating Services. A Maintenance Cyber Asset is not considered part of a BES Cyber System.

BES Cyber System Information

Information, about one or more BES Cyber Systems or BES Cyber Assets, that include one or more of the following: security procedures developed by the responsible entity; network topology or similar diagrams; BES Cyber System, Electronic Access Control System, and Physical Access Control System security configurations (e.g., network addresses, security patch levels, list of logical network accessible ports); floor plans that contain BES Cyber System Impact designations; equipment layouts that contain BES Cyber System Impact designations; BES Cyber System disaster recovery plans; and BES Cyber System incident response plans.

BES Reliability Operating Services

BES Reliability Operating Services are those services contributing to the real-time reliable operation of the Bulk Electric System (BES). They include the following Operating Services:

Dynamic Response to BES conditions

Actions performed by BES Elements, Facilities or systems automatically triggered to initiate a response to a BES condition. These actions are triggered by a single element or control device or a combination of these elements or devices in concert to perform an action or cause a condition in reaction to the triggering action or condition.

Aspects of BES Dynamic Response include, but are not limited to:

- Spinning reserve (contingency reserves)
  - Providing actual reserves
  - Monitoring that reserves are sufficient
- Governor Response
  - Control system used to actuate governor response

- Protection Systems (transmission & generation)
  - Line, bus, x-former, generator
  - Zone protection
  - Breaker protection
  - Current, frequency, speed, phase
- Special Protection Systems or Remedial Action Schemes
  - Sensors, relays & breakers, possibly software
- Under and Over Frequency relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Under and Over Voltage relay protection (includes automatic load shedding)
  - Sensors, relays & breakers
- Power System Stabilizers

Balancing Load and Generation

Activities, actions and conditions necessary for monitoring and controlling generation and load in the operations planning horizon and in real-time.

Aspects of the Balancing Load and Generation Operating Service include, but are not limited to:

- Calculation of ACE
  - Field data sources (real time tie flows, frequency sources, time error, etc)
  - Software used to perform calculation
- Unit commitment
  - Know generation status & capability & restrictions (must runs, minimum run times, ramp, heat rates, etc), load schedules
- Load management
  - Ability to identify load change need
  - Ability to implement load changes
- Demand Response
  - Ability to identify load change need
  - Ability to implement load changes
- Manually Initiated Load shedding
  - Ability to identify load change need
  - Ability to implement load changes
- Non-spinning reserve (contingency reserve)
  - Know generation status, capability, ramp rate, start time

- Start units and provide energy

Controlling Frequency (Real Power)

Activities, actions and conditions which ensure, in real time, that frequency remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Frequency Operating Service include, but are not limited to:

- Generation Control (such as AGC)
  - ACE, current generator output, ramp rate, unit characteristics
  - Software to calculate unit adjustments
  - Transmit adjustments to individual units
  - Unit controls implementing adjustments
- Regulation (regulating reserves)
  - Frequency source, schedule
  - Governor control system

Controlling Voltage (Reactive Power)

Activities, actions and conditions which ensure, in real time, that voltage remains within bounds acceptable for the reliability or operability of the BES.

Aspects of the Controlling Voltage Operating Service include, but are not limited to:

- AVR (Automatic Voltage Regulation)
  - Sensors, stator control system, feedback
- Capacitive resources
  - Status, control (manual or auto), feedback
- Inductive resources (transformer tap changer, or inductors)
  - Status, control (manual or auto), feedback
- SVC (Static VAR Compensators)
  - Status, computations, control (manual or auto), feedback

Managing Constraints

Activities, actions and conditions that are necessary to ensure that elements of the BES operate within design limits and constraints established for the reliability and operability of the BES.

Aspects of the Managing Constraints include, but are not limited to:

- Available Transfer Capability (ATC)

- Interchange schedules
- Generation re-dispatch and unit commit
- Identify and monitor SOL's & IROL's

Identify and monitor Flowgates

Monitoring & Control

Activities, actions, and conditions that provide monitoring and control of BES elements.

An example aspect of the Monitoring and Control Service is, but is not limited to:

- All methods of operating breakers and switches (such as SCADA)

Restoration of BES

Activities, actions and conditions necessary to go from a shutdown condition to an operating condition delivering electric power without external assistance.

Aspects of the Restoration of BES Operating Service include, but are not limited to:

- Blackstart restoration including planned cranking path
- Off-site power for nuclear facilities.

Situational Awareness

Activities, actions and conditions necessary to assess the current condition of the BES and anticipate effects of planned and unplanned changes to conditions.

Aspects of the Situation Awareness Operating Service include, but are not limited to:

- Monitoring and alerting (such as EMS alarms)
- Change management
- Current Day & Next Day planning
- Contingency Analysis
- Frequency monitoring

Inter-Entity Real-Time Coordination and Communication

Activities, actions, and conditions necessary for the coordination and communication between Responsible Entities to ensure the reliability and operability of the BES.

Aspects of the Inter-Entity Coordination and Communication Operating Service include, but are not limited to:

- Scheduled interchange
- Facility operational data and status
- Operational directives

CIP Exceptional Circumstance

A situation that involves one or more of the following conditions: a risk of injury or death, a natural disaster, civil unrest, 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 the requirements within the NERC CIP Standards.

Control Center

One or more facilities hosting a set of one or more BES Cyber Assets or BES Cyber Systems performing one or more of the following functions that support real-time operations by System Operators for two or more BES generation facilities or transmission facilities, at two or more locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,
- Inter-utility exchange of BES reliability or operability data,
- Providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES,
- Alarm monitoring and processing specific to the reliable operation of the BES and BES restoration function,
- Presentation and display of BES reliability or operability data for monitoring, operating, and control of the BES
- Coordination of BES restoration activities.

Cyber Assets

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

Defined Physical Boundary ("DPB")

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.

Change Rationale: "Defined Physical Boundary (DPB)" replaces "Physical Security Perimeter." *Previous versions of the CIP standard focused on the development of a completely enclosed Physical Security Perimeter (PSP) ("six-wall" border) and managing access though this boundary. This has proven difficult due to the nature of the operating environment for many electrical utilities, especially in field locations. The intent of this standard is to focus on the controls put in place to restrict access rather than solely focusing on the PSP and a boundary protection model for physical security.*

Electronic Access Control or Monitoring Systems

Cyber Assets used in the access control or monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems

Electronic Access Point ("EAP")

An interface on a Cyber Asset that restricts routable or dial-up data communications between Cyber Assets.

Electronic Security Perimeter ("ESP")

~~The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.~~
A collection of Electronic Access Points that protect one or more BES Cyber Systems.

External Connectivity

Routable or dial-up data communication through an Electronic Access Point between a BES Cyber Asset and a device external to the Electronic Security Perimeter.

External Routable Connectivity

The BES Cyber System is accessible from any Cyber Asset that is outside its associated ESP via a routable protocol.

Interactive Remote Access

Any user interactive access by a person that 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 network-based or dial-up access. Remote access can be initiated from: 1) Cyber Assets used by the Responsible Entity, 2) Cyber Assets used by employees, and 3) Cyber Assets used by vendors, contractors, or consultants.

Intermediate Device

A Cyber Asset that 1) may be used to provide the required multi-factor authentication for the interactive remote access; 2) may be a termination point for required encrypted communication; and 3) may restrict the interactive remote access to only authorized users. Intermediate devices are sometimes called proxy systems. The functions of an intermediate device may be implemented on one or more Cyber Assets. The intermediate device may be located outside the Electronic Security Perimeter, as part of the Electronic Access Point, or in a DMZ network.

Physical Access Control Systems

Cyber Assets that control, alert, or log access to the Defined Physical Boundary(s), exclusive of locally mounted hardware or devices at the Defined Physical Boundary such as motion sensors, electronic lock control mechanisms, and badge readers.

Protected Cyber Asset

A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the BES Cyber System. A Transient Cyber Asset is not considered a Protected Cyber Asset.

Reportable BES Cyber Security Incident

Any BES Cyber Security Incident that has compromised or disrupted a BES Reliability Operating Service.

Transient Cyber Asset

A Cyber Asset that is: 1) directly connected for 30 calendar days or less to a BES Cyber Asset or Protected Cyber Asset, 2) used for data transfer, maintenance, or troubleshooting purposes, and 3) capable of altering the configuration of or introducing malicious code to the BES Cyber System.

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

Physical Security Perimeter