Pacific Northwest
NATIONAL LABORATORY

PNNL-SA-204388

NERC CIP and Cloud Services

October 16, 2024

Scott R. Mix, CISSP
Grid Cybersecurity Specialist

U.S. DEPARTMENT OF ENERGY BATTELLE

PNNL is operated by Battelle for the U.S. Department of Energy

Pacific Northwest
NATIONAL LABORATORY

Agenda

- Introduction
- NERC Standards Focus
- NERC CIP Definitions
- Impact on Cloud Services
- Other and Future Activities
- Possible Solutions
- Questions

NERC Standards Focus

- NERC Standards apply to the Bulk Electric System (BES)
  - Generally, 100kV and above, but with some exceptions, primarily for radial lines
  - 20MVA and above generating units, 75MVA and above generating plants, with some exceptions for wholly behind-the-meter generation
    - ✓New rules for IBR
  - Includes Control Centers that monitor and control the BES
- Scoped and Bounded by NERC definitions*
  - Specifically, the BES Cyber Asset definition
- NERC Standards do not apply to distribution (i.e., non-BES)
  - With several exceptions: primarily UFLS, UVLS, Blackstart Resources (generation), Cranking Paths

* See https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Definitions

- ***Cyber Asset***: Programmable electronic devices, including the hardware, software, and data in those devices.
- ***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.

Definitions

- ***Cyber Asset***: Programmable electronic devices, including the hardware, software, and data in those devices.
- ***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.

Emphasis added

Definitions

- **Cyber Asset**: Programmable electronic devices, including the hardware, software, and data in those devices.
- ***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.

Emphasis added

Definitions

- ***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.
  - Components of the BCS also include “glue” infrastructure components (e.g., networking infrastructure) necessary for the system to perform its reliability tasks, like network switches
  - Tremendous flexibility is built into the definition – BCS could be the entire control system, or a subset based on function (HMI, server, database, FEP, etc.)
- ***Electronic Security Perimeter (ESP)***: The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
  - Term “network” is not clearly defined – assume it is a physical network

Definitions

- ***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.
  - That is, *any* computer node (Cyber Asset) that is on the same network as a BES Cyber System
  - From ESP definition - term “network” is not clearly defined – assume it is a physical network

Pacific Northwest
NATIONAL LABORATORY

Definitions

- ***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 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.
- ***Physical Access Control Systems (PACS)***: Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Definitions

- ***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 tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
  - Includes rooms and equipment where power system operators sit, as well as rooms and equipment containing the “back office” servers, databases, telecommunications equipment, etc.
  - They may all be in the same room or be located in different buildings or in different cities.

Definitions

- ***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 tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
  - Includes rooms and equipment where power system operators sit, as well as rooms and equipment containing the “back office” servers, databases, telecommunications equipment, etc.
  - They may all be in the same room or be located in different buildings or in different cities.
  - Note – nothing stated about ownership or physical location in relation to the utility

Emphasis added

Definitions

- ***BES Cyber Systems Information***: Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the 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 BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, 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 BCS.

Pacific Northwest
NATIONAL LABORATORY

Impact on Cloud Services

- CIP definitions are “device” centric
  - That is, the physical computers that make up the cloud computing infrastructure
- BCAs / BCSs perform “real-time” functions of monitoring or controlling the BES
  - Includes core networking infrastructure and network attached storage necessary to perform functions (they are “programmable electronic devices”)
  - Since the cloud implementation allows application processing to occur on different compute nodes depending on availability, virtually all computers in the cloud could (would) be considered BES Cyber Assets
    - ✓Cloud providers may be able to restrict nodes that can perform BES functions to a limited subset of cloud infrastructure, but one significant advantage of cloud services is the ability to migrate functions to other nodes to increase processing capability or in the event of failure

Impact on Cloud Services

- BCAs / BCSs in the cloud performing Control Center functions makes the cloud part of the defined the Control Center
  - Cloud-resident services performing protection and control functions in or providing critical telemetry from a BES substation makes the cloud systems hosting those functions BCAs or BCSs
- BCAs / BCSs connected to a network must be surrounded by an ESP
  - Likely the “cloud border” since the ESP must contain all computers that could meet the definition of a BCA, or that could perform the BCA’s functional processing
    - ✓Recall the “when needed” clause in the BCA definition
  - Cloud border infrastructure (routers, firewalls, etc.) would be considered EACMS devices, and contain EAPs

Impact on Cloud Services

- Other Cyber Assets inside the ESP are likely, at minimum, PCAs
  - All the other computers in the cloud (i.e., inside the ESP / cloud boundary) – even if configured to not execute your applications
- There is no exclusion consideration for location, ownership, or other use of Cyber Assets
  - All computers, network access points, users, etc. of the cloud, regardless of who owns them or uses them, are therefore subject to your compliance obligations
- Many of the CIP requirements apply both to BCS/BCAs and PCAs
- Audits may be able to rely on “work of others”, but those other audits typically do not cover all the requirements in a CIP audit – specifically any “entity-specific” requirements

Impact on Cloud Services

- CIP-004-7, R2 (formal training), R3 (personnel risk assessments) and R4 (access authorization)
  - All personnel with electronic or physical access to BES Cyber Systems, PACS, and EACMS must undergo entity specific (or at least entity approved) training, entity defined PRA, and be individually authorized by the entity

Impact on Cloud Services

- CIP-004-7, R2 (formal training), R3 (personnel risk assessments) and R4 (access authorization)
  - All personnel with electronic or physical access to BES Cyber Systems, PACS, and EACMS must undergo entity specific (or at least entity approved) training, entity defined PRA, and be individually authorized by the entity
    - ✓The standards do not restrict these requirements to only entity employees – they are specifically broad to include vendors and contractors
    - ✓Would apply to cloud service provider staff as well as staff from other cloud tenants using the same hardware or are on the same network

Emphasis added

Impact on Cloud Services

- CIP-005-7 Requirement 1 (ESP and border protections)
  - All traffic crossing the ESP in either direction must be authorized, with rationale for granting access, and traffic must be inspected for known or suspected malicious activities

Impact on Cloud Services

- CIP-005-7 Requirement 1 (ESP and border protections)
  - All traffic crossing the ESP in either direction must be authorized, with rationale for granting access, and traffic must be inspected for known or suspected malicious activities
    - ✓Not just your traffic, or just traffic to your systems
    - ✓Would include traffic for all other cloud tenants that use the hardware, or are on the same network

Emphasis added

Pacific Northwest
NATIONAL LABORATORY

Impact on Cloud Services

- CIP-006-6 Requirement R1 (physical security perimeters)
  - All medium impact BES Cyber Systems with External Routable Connectivity must utilize at least one physical access control to restrict access to personnel individually authorized by the entity
  - All high impact BES Cyber Systems with External Routable Connectivity must utilize at least two physical access control to restrict access to personnel individually authorized by the entity
  - Monitoring and alarming required (and visible to the entity)

Impact on Cloud Services

- CIP-007-6 R2 (patching)
  - All high and medium impact BES Cyber Systems, PCAs, and EACMS must have a patch management program to analyze patches at least every 35 days, and install or mitigate all patched vulnerabilities within 35 days of the completion of the analysis

Impact on Cloud Services

- CIP-007-6 R2 (patching)
  - All high and medium impact BES Cyber Systems, PCAs, and EACMS must have a patch management program to analyze patches at least every 35 days, and install or mitigate all patched vulnerabilities within 35 days of the completion of the analysis

Emphasis added

Impact on Cloud Services

- CIP-007-6 R4 (event monitoring)
  - All high and medium impact BES Cyber Systems, PCAs, and EACMS must have security event monitoring, including alerting, log retention, and a process to identify undetected Cyber Security Incidents (high impact)

Impact on Cloud Services

- CIP-007-6 R4 (event monitoring)
  - All high and medium impact BES Cyber Systems, PCAs, and EACMS must have security event monitoring, including alerting, log retention, and a process to identify undetected Cyber Security Incidents (high impact)
  - Expectation is that the monitoring and alerts are visible to the entity
  - An entity-managed SIEM (security information and event management) system could be used to collect event data

Emphasis added

Other and Future Activities

- Work is underway to address the use of Cloud Services within the NERC CIP environment
  - Project 2016-02 Modifications to CIP Standards (Virtualization) – Filed with FERC
  - Project 2019-02 BES Cyber System Information Access Management – Filed with FERC
  - Project 2023-09 Risk Management for Third-Party Cloud Services – proposed
- Whitepaper on BES Operations in the Cloud (not a standards document)

Project 2016-02 New Definitions

- ***Virtual Cyber Asset (VCA):*** 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.

Project 2016-02 New Definitions

- ***Shared Cyber Infrastructure (SCI):*** 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 System (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.
  - **Essentially – the cloud service provider's systems are now categorized as SCI – and therefore included within the scope of the CIP standards**

Project 2016-02 Changes

- Adds VCA and SCI language alongside BCS, BCA, PCA language in many definitions and requirements
  - For example: new definition for **BES Cyber Asset**: 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 (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.
  - CIP-004-8 R2 adds SCI to applicable systems column for Security Training program
  - CIP-007-7 R1 adds SCI to applicable systems for “system hardening”
  - CIP-007-7 R2 adds SCI to patch requirements
  - CIP-008-7 R1 adds SCI to Cyber Security Incident Response Plan

Project 2016-02 Changes

- Adds VCA and SCI language alongside BCS, BCA, PCA language in many definitions and requirements
  - For example: new definition for **BES Cyber Asset**: 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 (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.
  - CIP-004-8 R2 adds SCI to applicable systems column for Security Training program
  - CIP-007-7 R1 adds SCI to applicable systems for “system hardening”
  - CIP-007-7 R2 adds SCI to patch requirements
  - CIP-008-7 R1 adds SCI to Cyber Security Incident Response Plan

Emphasis added

Project 2019-02 Changes

- Modified provisions in CIP-004 and CIP-011 to account for off-site electronic storage of BCSI
  - Allows cloud storage of BCSI

Possible Solutions

- Utilize cloud environments for applications where the Cyber Assets *do not* meet the definition of a BES Cyber Asset / System or an EACMS:
  - Not used in “15-minute” decision-making processes
  - Long-term planning studies
  - Secondary SIEM processing (primary log analysis is performed on an EACMS)
  - Support services, such as help-desk, ticketing systems, work order processing
  - Market functions
  - Distribution
- Be aware of BCSI protection requirements, which are less stringent than those required for BES Cyber Systems, but need to be followed

Pacific Northwest
NATIONAL LABORATORY

Questions

Pacific Northwest
NATIONAL LABORATORY

Thank you

Scott R. Mix, CISSP
Grid Cybersecurity Specialist
scott.mix@pnnl.gov