NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2023-03 INSM

INSM Standards Drafting Team Member
Industry Webinar
January 3, 2024

RELIABILITY | RESILIENCE | SECURITY




Administrative

- North American Electric Reliability Corporation (NERC) Antitrust Guidelines
  - It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition

Limited Disclosure

Agenda

- Standards Drafting Team (SDT)
- Background
- Interpretation of the Term CIP-Networked Environment
- INSM Comments
- CIP-007-X Revisions: R6 (Parts 6.1-6.7)
- Q&A
- SDT Contact Information

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team

Name	Entity
Thad Ness, Chair	NextEra Energy
Valerie Ney, Vice Chair	FirstEnergy Corporation
Joseph Jimenez	Duke Energy
Dan Toth	American Transmission Company, LLC
Mark Johnson-Barbier	Salt River Project
Erin Wilson	New Brunswick Power
Robert Rinish	PPL Electric Utilities
Aaron Williams	Southern Company
Eric Rupp	Great River Energy
Alan Kloster	Evergy, Inc.
Darcy Guenette	Ontario Power Generation
Tim McDonald	PG&E
David Crim	MISO

Background

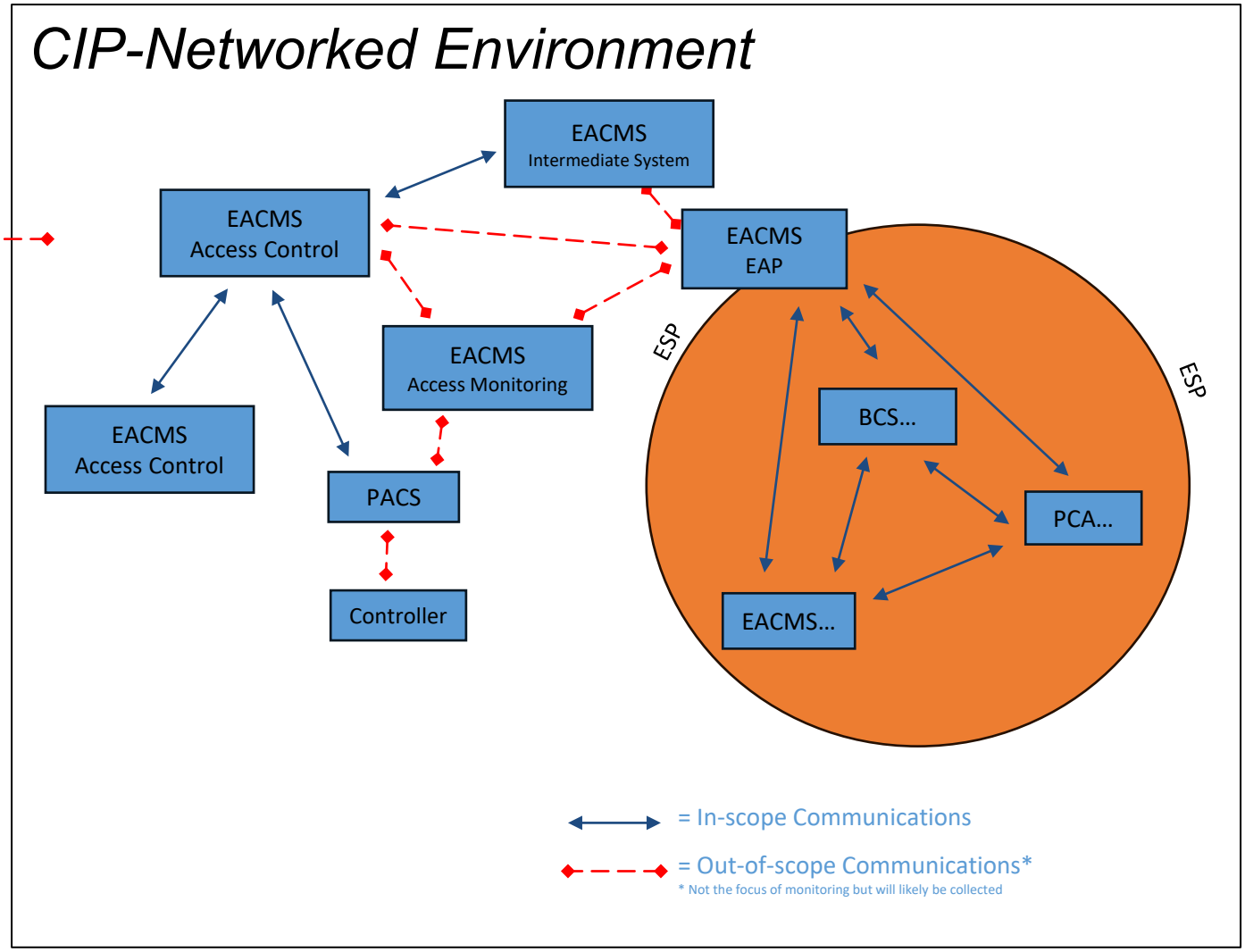
- INSM permits entities to monitor traffic within a trusted zone (e.g., ESP) to detect intrusions or malicious activity.
- January 19, 2023 – FERC Order No. 887 directed NERC to:
  - Develop requirements within CIP Reliability Standards for INSM
    - High-impact Bulk Electric System (BES) Cyber Systems
    - Medium impact BES Cyber Systems with External Routable Connectivity (ERC)
  - FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.
- Reliability Standard CIP-007-X
- Correlation of Reliability Standards CIP-007-X and CIP-008-6

Limited Disclosure

Background

- FERC Order No. 887 – Key Dates
  - Effective: 10 April 2023
  - Final Report: 9 July 2024
- Internal Network Security Monitoring (INSM)
  - Applied within a trust zone (e.g., ESP)
  - Trust zone is “CIP-networked environment”
  - Activity that has circumvented perimeter controls

Interpretation of the Term "CIP-networked environment"



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Interpretation of the Term "CIP-networked environment"

- CIP-networked environment in the context of Project 2023-03 includes:
  - ESP(s) associated with:
    - High Impact BES Cyber Systems and their associated PCAs
    - Medium Impact BES Cyber Systems with ERC and their associated PCAs
  - Routable communications between
    - EACMS (either internal or external to the ESP) associated with High Impact BES Cyber Systems
    - EACMS and PACS associated with High Impact BES Cyber Systems
    - EACMS (either internal or external to the ESP) associated with Medium Impact BES Cyber Systems with External Routable Connectivity
    - EACMS and PACS associated with Medium Impact BES Cyber Systems with ERC
  - CIP devices (BCS, EACMS, PACS and PCAs) only
  - Communications between a PACS and EACMS (communications between a PACS and any other device is out of scope)

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

INSM Comments

- System Classification Options
  - No INSM designation – BCSI or EACMS protections will be utilized
- SDT anticipates that INSM Systems will be designated either:
  - BCSI Repository
    - Most standalone INSM systems
  - EACMS
    - If combined with SIEM that does access monitoring
    - INSM limitations related to access monitoring

Limited Disclosure

CIP-007-X Revisions: R6

- CIP-007-X R6.
  - *Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-X Table R6 – Internal Network Security Monitoring (INSM) to increase the probability of detecting an attack that has bypassed other security controls. – [Violation Risk Factor : Medium] [Time Horizon: Same Day Operations and Operations Assessment].*
- M6.
  - Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts of CIP-007-X Table R6 – INSM and additional evidence to demonstrate implementation as described in the Measures column of the table.

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.1

CIP-007-X Table R6 – INSM			
Part	Applicable Systems	Requirements	Measures
6.1	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.	Examples of evidence may include, but are not limited to, architecture documents or other documents detailing data collection locations and methods

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.1

- Requirement R6.1
  - Identify network data collection locations and methods that provide visibility of network communications (excluding serial) between applicable Cyber Assets to monitor and detect anomalous activity, including connections, devices, and network communications. 100 percent coverage is not required. Collection methods should provide security value to address the perceived risks.
- Not Prescriptive
  - Too many architectures and edge cases
  - Responsible entities will have collection design and then defend it
  - Technical Rationale will provide more guidance
- Some Level of INSM Network Collection
  - Full PCAP (TAP, SPAN)
  - Remote collection (RSPAN, Net Flow)
  - SDN logs
  - Other options

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.1

- Vendor Support
  - Historical "vendor not supported" → cybersecurity monitoring is changing
  - Responsible entities may need to purchase modern equipment
  - There is no "per system capability", but 100% collection is not required
  - You can work around supportability concerns

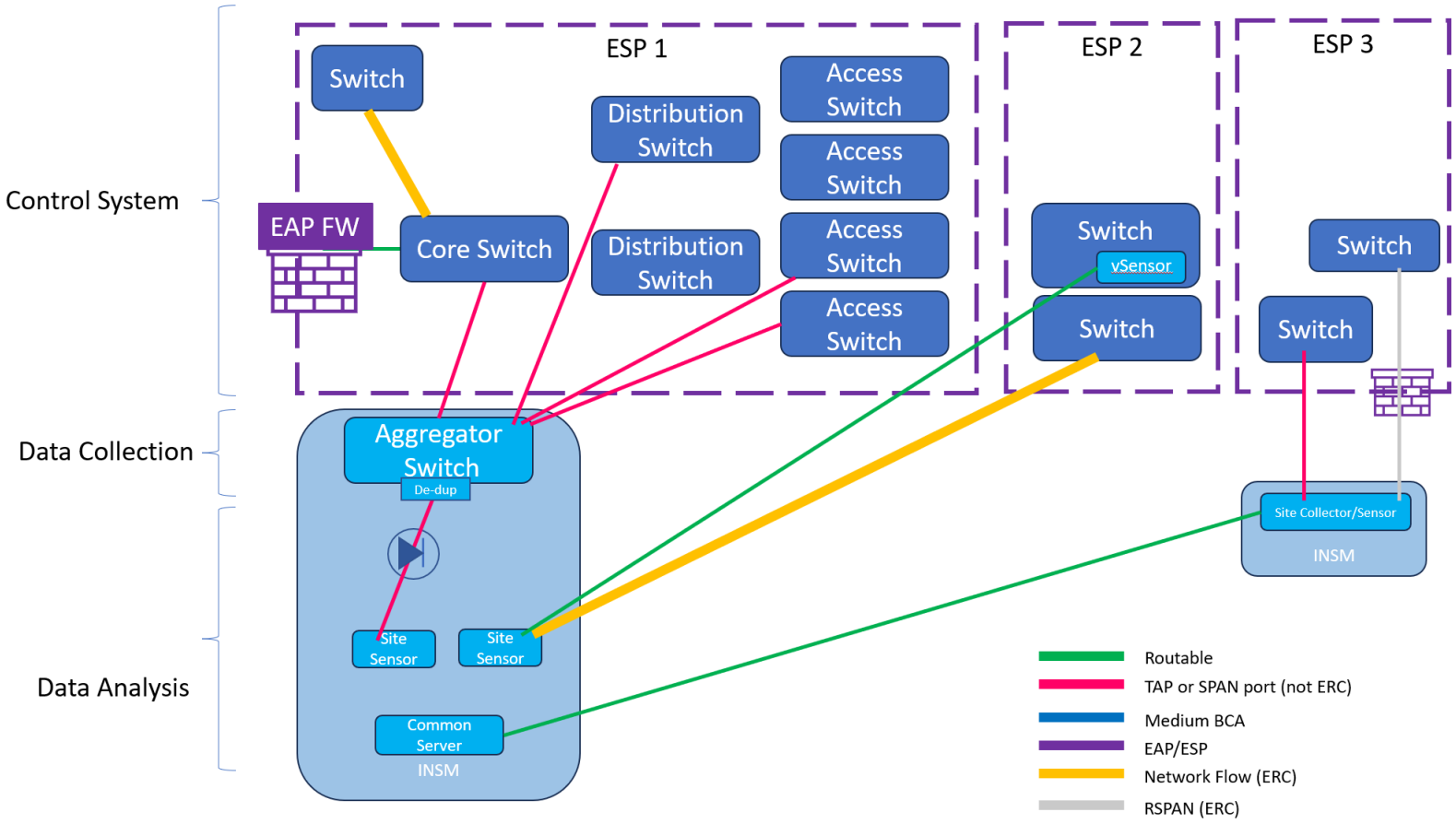
- Collection – Balance
  - Identify convergence locations
  - Start Collection to gather higher value
  - Tune/add/remove over time
  - Layer 2 collection in some locations
  - Layer 3 collection in some locations
  - Balance with other capabilities (SIEM/Endpoint/EDR)

> *"He who defends everything, defends nothing."*
>
> *Attributed to Fredrick the Great*

Limited Disclosure

CIP-007-X Revisions: R6.1

Reference Architecture



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.2

6.2	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Log collected data regarding network communications at the network locations identified in Part 6.1.	An example of evidence is data collected from the identified network locations in Part 6.1.

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.2

- Requirement 6.2
  - *Log collected data regarding network communications at the network locations identified in Part 6.1.*
- Collect and Log Data
  - Expect Continuous collection
  - Keep a record of the data
    - Full PCAP – acceptable but not required
    - Summarized data (what all the tools do – data summarized into database/visualization tool)
- Use Cases
  - Threat hunting
  - “Weird Traffic” – where to start a hunt
  - Investigations

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.3

6.3	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Evaluate the collected data to document the expected network communication baseline.	Examples of evidence should include documented expected network communication or other representation(s) of expected network communication.

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.3

- Requirement R6.3:
  - *Evaluate the collected data to document the expected network communication baseline.*
- What is a "baseline"?

A baseline is…	A baseline is not…
Record of observed traffic	A spreadsheet listing all expected traffic
Continuously updated by a computer	Updated infrequently by a person
Searchable database	Point-in-time list
Assets that have communicated on the network	A spreadsheet of assets made by an intern or engineer

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.4

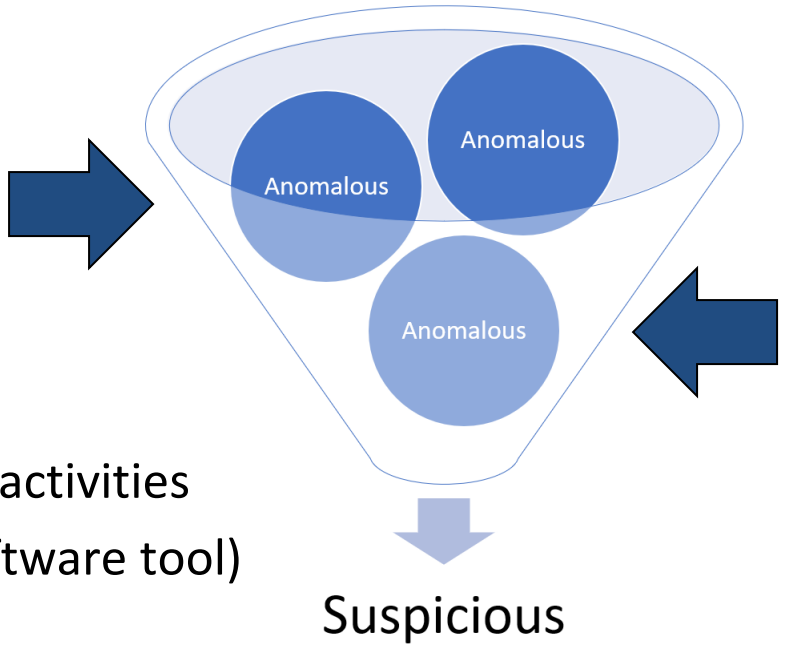
6.4	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.	Examples of evidence may include, but are not limited to, a paper or system generated list of detected anomalous activity or detection configuration.

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.4

- Requirement R6.4:
  - *Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2.*
- No specific technology required
  - "Anomalous" != "anomaly detection"
  - Tools generate a lot of notifications
- Methods:
  - Threat hunting
  - Signature based alerts
  - Correlation of signatures with other logged activities
  - Anomaly detection (usually defined by a software tool)
  - Artificial Intelligence and machine Learning
  - Other proprietary and open-source methods



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

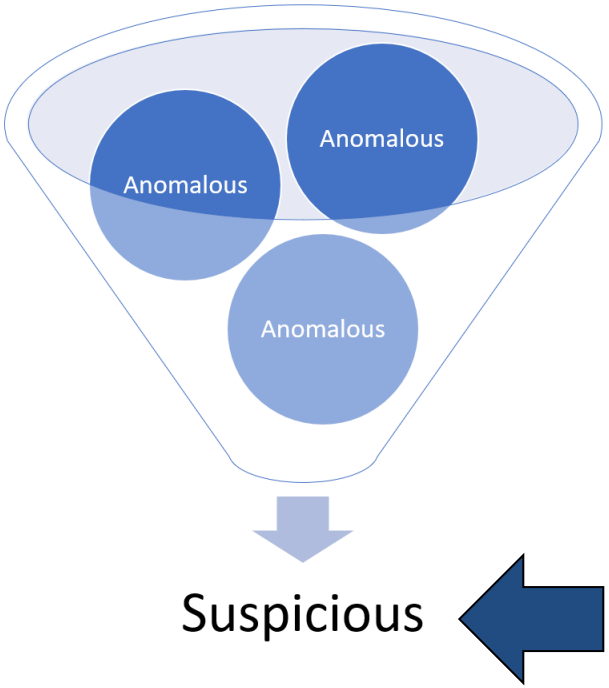
CIP-007-X Revisions: R6.5

6.5	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.	Examples of evidence may include, but are not limited to, documentation of criteria used to evaluate anomalous activity; documentation of responses to detected anomalies, etc.

Limited Disclosure

CIP-007-X Revisions: R6.5

- Requirement R6.5:
  - *One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action.*
- Use notifications from R6.4
  - Look for the “needle”
  - May not indicate CIP-008 escalation



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.6

6.6	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.	Examples of evidence may include, but are not limited to, documentation of the data retention process and paper or system generated reports showing data retention configuration with timelines sufficient to perform the analysis of anomalous activity.

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.6

- Requirement R6.6:
  - *Develop one or more method(s) to retain network communications data and other relevant data collected with sufficient detail and duration to support the investigation of anomalous activity.*
- "Maintain" ~= "Retention"
- Responsible entities determine what data to retain and for how long
- Likely Retention Options:
  - PCAP retention (payload data): seconds-days
    - Encrypted payloads: extremely low retention value
    - May choose to retain payloads of value
      - PCAP related to an alert/suspected attack
      - Operational information
  - Summary data: commonly retained 3-6 months
  - CIP-008 timeframes will likely apply

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Revisions: R6.7

6.7	High Impact BES Cyber Systems and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA. Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: 1. EACMS that perform access control functions; 2. PACS that rely upon EACMS that perform access control functions; and 3. PCA.	One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.	Examples of evidence may include, but are not limited to, documentation demonstrating how data is being protected from the risk of deletion or modification by an adversary. ~~b R6, Part~~

Limited Disclosure

CIP-007-X Revisions: R6.7

- Requirement R6.7:
  - *One or more process(es) to protect the data collected in Part 6.2 to mitigate the risks of deletion or modification by an adversary.*
- From Order 887:
  - "Minimize the likelihood of an attacker removing evidence of TTPs from compromised devices."
  - Controls for protecting BCSI and EACMS are probably sufficient
- R6.7 is NOT about limiting information sharing with partners and vendors.
  - INSM data needs to be shared as part of a mature security monitoring program
  - This includes IP addresses

Limited Disclosure

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Implementation Plan

- CIP-007-X
  - Approval by an applicable governmental authority is required
    - **first calendar quarter that is thirty-six (36) months after the effective date of the applicable governmental authority's order approving the standard**, or as otherwise provided for by the applicable governmental authority.
  - Approval by an applicable governmental authority is not required
    - **first day of the first calendar quarter that is thirty-six (36) months after the date the standard is adopted by the NERC Board of Trustees**, or as otherwise provided for in that jurisdiction

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-007-X Requirement R6 Implementation Plan

- Requirement R6
  - All Responsible Entities with applicable systems located at Control Centers and backup Control Centers identified pursuant to CIP-002-5.1(a) Requirement R1.1 and R1.2 shall initially comply with the requirements in CIP-007-X Requirement R6 for those Control Centers upon the effective date of Reliability Standard CIP-007-X. This implementation timeframe recognizes the increased reliability risk posed by high impact BES Cyber Systems, Control Centers, and backup Control Centers. It further accommodates for the challenges posed by the limited pool of vendors, time required to identify and implement data feeds, the analysis of results and necessary testing, and adjustments for the implementation of INSM.
  - All Responsible Entities with applicable systems located at medium impact BES Cyber Systems with External Routable Connectivity, with the exception of Control Centers and backup Control Centers discussed above, shall be required to apply CIP-007-X Requirement R6 within 24 calendar months after the effective date of Reliability Standard CIP-007-X.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Questions and Answers

Q & A

- Are EACMS/PACS communications in scope?
  - Yes
- Informal Discussion
  - Via the Questions and Answers feature.
  - Respond to stakeholder questions.
- Other
  - Some questions may require future SDT consideration.
  - Please reference slide number, standard section, etc., if applicable.
  - SDT will address as many questions as possible.
  - Webinar and chat comments are not a part of the official project record.
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the SDT.

Limited Disclosure

Project 2023-03 INSM Contact Information

- Point of Contact
  - Laura Anderson, Standards Developer
    - laura.anderson@nerc.net or call 404-782-1870
- Webinar Slides and Recording Posting
  - Within 24-72 hours of Webinar completion
  - Link will be available in the Standards, Compliance, and Enforcement Bulletin

Limited Disclosure