NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Technical Rationale for Reliability Standard CIP-007-X

## CIP-007-X – Cyber Security – System Security Management

## Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-007-X. It also provides guidance to responsible entities for clarifying Internal Network Security Monitoring (INSM) systems and the original intent of the Standard Drafting Team (SDT). This Technical Rationale document for CIP-007-X is not a reliability standard and should not be considered mandatory and enforceable.

## Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address the three security issues.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

## Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats and incidents. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

The Project 2023-03 SDT proposed Reliability Standard CIP-007-X requires responsible entities to implement an NSM system. Responsible Entities will be required to collect, analyze, and respond appropriately to unexpected, anomalous, or otherwise suspicious network communications within applicable networks.

---

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following security issues: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

Responsible Entities are to evaluate their networks and identify the collection locations and methods most effective for their network configurations. Responsible entities will monitor and respond to anomalous communications and escalate these occurrences, if appropriate. Responsible entities will also appropriately protect NSM systems and data. In order to assist other entities and improve the nationwide security of electric systems, responsible entities are encouraged to share NSM data with technical and security support groups and peers: including law enforcement; defense organizations, such as the CISA; and industry partners and vendors. NSM will be an on-going, or possibly an iterative, process enabling responsible entities to actively identify, mitigate, and escalate threatening actions before they are allowed to impact the reliable operation of the BES.

INSM [i-en-es-em] is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of systems that are internal to the operational zones of the entity, and also includes associated systems; such as Physical Access Control Systems (PACS), access monitoring systems, and Electronics Access Control Systems (EACMS). While the entities are encouraged to use NSM systems at other critical networks, such as corporate internet perimeters, these requirements apply only to the applicable systems listed in the standard.

# General Considerations

## Regulatory changes to CIP-007, CIP-005, or a new standard

The SDT considered several options regarding the addition of INSM requirements to the CIP framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887[3], schedule expectations, and the fundamental principles of NSM as detailed in several books, such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4]; and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

The SDT concluded that INSM requirements would best align as an addition to Reliability Standard CIP-007 since the outcomes of INSM most closely align with management of security systems, particularly regarding collection and analysis of system data. INSM is a distinct function independent of the logging requirements already established in Reliability Standard CIP-007; but taken together, INSM and the pre-existing Reliability Standard CIP-007 requirements complement each other in helping responsible entities improve overall management of security systems.

## System Classification

INSM systems will not carry a specific CIP term; such as Electronic Access Point (EAP) or EACMS. INSM systems, and some INSM components, may be classified as BES Cyber Systems Information Repositories (BCSI) or EACMS. INSM systems are commonly classified as BCS Information Repositories, which is an acceptable designation.

[3] *Id.*
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

An entity may choose to classify a standalone INSM system as an EACMS, but the entity should be aware that an INSM system using only network traffic cannot precisely determine if an encrypted login attempt is failed or successful (example encrypted protocols include ssh, https, RADIUS, and RDP). INSM systems may attempt to infer login success or failure using network data, such as session duration and amount of data transferred. Because of this limitation, INSM systems are a poor choice for monitoring and alerting on successful and failed electronic access when using encrypted protocols. Detection of events, such as failed and successful logons, is more precise when supplemented with endpoint logs.

**Classification Rationale**

INSM systems, as well as the networks they are monitoring, can be configured in a very wide array of possibilities. As such, the system classifications could also vary depending on the design implemented by the responsible entity. Ideally, INSM systems are segmented from the network components being monitored, as well as from the enterprise business network. Network communications very often also do not obviously contain physical location details for the assets joined to the network, but having this information readily available in the NSM system will make the system much more usable for the responsible entity. NSM system input data is most often duplicated network communication streams, copied through the use of a dedicated device, like a network tap, or through use of network switch port mirroring. Other options exist as well, such as using an endpoint device to collect and transfer duplicated network communication. All of these methods require transferring duplicated traffic to the NSM system via non-routable protocols, such as those sourced from a network tap or mirrored port, or it involves the transfer of duplicated data through the use of a routable protocol from an end device serving as a collector or monitoring sensor.

This traffic can all be securely sent outside of the primary CIP-networked environments being monitored. Ideally, the NSM system would only be designated as a BCSI; although portions, such as end point collectors, could be classified as Protected Cyber Assets (PCAs). Similarly, the responsible entities could designate INSM systems as an EACMS, however the intent of the SDT is that NSM focuses primarily on the collection, analysis, and response to abnormal network traffic. Collection of BCS alerts, logging, and authentication is best handled elsewhere.

Responsible entities are intended to leverage EACMS data, as well as any other pertinent information, to help provide context during analysis of network anomalies identified through INSM. Addition of INSM is not intended to replace or detract from the functions and requirements applied to EACMS.

**INSM**

The goal of INSM is to detect adversarial activity. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as Endpoint Detection and Response (EDR). By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While an entity may choose to implement active prevention measures in an INSM system, prevention is not expected in this requirement.

The principles of INSM as defined in Richard Bejtlich's book, *The Practice of Network Security Monitoring*, can be summarized in three main actions: collect, analyze, and escalate. The outcome of INSM is to establish an independent collection and monitoring system enabling cyber defenders to identify and respond appropriately to network activity caused by threat actors in preparation of an attack. Threat actors commonly take steps to hide their actions, and very often need to work for an extended period within targeted environments to develop disruption capabilities.

During successful cyber-attacks, these preparatory actions often go unnoticed. NSM Monitoring establishes capabilities to detect these actions independent of all the other security controls that are already in place. This enables defenders to take corrective actions to prevent and disrupt attacks prior to disruption. To be effective, NSM needs to maintain independence of monitored systems to avoid common modes of failure.

### Vendor Support

The SDT is aware that some control system vendors have historically stated that their systems do not support cybersecurity monitoring using either INSM data collection or endpoint logging collection. The INSM collection requirements do not include the statement “per system capability” specifically because it is the intent of the SDT that every control system should have the capability to provide an appropriate level of visibility.

Requirement R6, Part 6.1 allows wide latitude to design supported cybersecurity data collection systems and allows vendors the option to gather cybersecurity information at the network and endpoint. Many control systems generate logs with relevant cybersecurity information, such as asset configuration, version levels, and access logs. A vendor-supported logging system may include forwarding existing logs to a cybersecurity monitoring tool, which could augment the INSM collection system.

Industry experience has found that many vendor statements disavowing support for INSM or endpoint logging are based on the existence of outdated hardware or low-capacity hardware in the control system. To resolve capacity issues, entities may need to install modern equipment capable of supporting the deterministic needs of the control system and excess capacity to support cybersecurity collection systems such as INSM or endpoint logging agents.

### Information Sharing

A mature security monitoring program requires sharing of information with partners; including government, utility, and industry stakeholders. No part of these requirements should be interpreted to limit or restrict responsible entities from continuing maturity of their information sharing programs. Data components that are collected by INSM systems may be shared with government, industry, and utility partners and vendors. Specifically allowed for sharing are packet capture files, network traces, and other network metadata including internal IP addresses that could benefit other Registered Entities and partners. When sharing information, responsible entities may redact unnecessary components from shared data, such as SNMP community strings and unencrypted logins.

Entities are encouraged to participate with mature information sharing programs and partnerships.

# Rationale for the Applicable Systems Section for Requirement R6 Parts

## Summary

NSM can be a very powerful tool for defense teams protecting critical functions, though it does have limitations. Understanding these strengths and weaknesses in context of the networks supporting BCS produced the "Applicable Systems" of the Requirement R6 parts.

Draft 1 of proposed CIP-007-X applies to high impact BCS and medium impact BCS environments that also have ERC. Isolated medium impact environments, or medium impact environments that only utilize serial communications, are exempt. Associated PCAs in high and qualifying medium impact environments are also included.

Draft 1 of proposed CIP-007-X applies to PACS and EACMS that are contained within or on the perimeter of a CIP high or qualifying medium impact environment. CIP-007-X also applies to network communications between EACMS and PACS that is applicable to assets inside of qualifying CIP high or medium impact environments.

INSM is primarily focused on internal network communications within these protected environments, and that includes communication that has traversed the EAP. INSM also applies to EACMS and PACS related to, but outside of, qualifying CIP high and medium environments due to the possibility of a threat actor need to manipulate such external systems in order to gain access to the protected environments.

The intention of the SDT is not that all communications outside of the qualifying environments be included in INSM; particularly, the encrypted traffic that has exited a protected zone, or the entirety of enterprise business networks. The diagram below helps illustrate this intent.

## CIP-networked environment

The term CIP-networked environment used in the context of standards development in support of project 2023-03 (Internal Network Security Monitoring) shall be inclusive of the following (adjusted for clarity for the purposes of showing SDT development of revisions to CIP-007-X):

- ESP(s) associated with High Impact BES Cyber Systems and their associated PCAs
- Routable communications between EACMS (either internal or external to the ESP) associated with High Impact BES Cyber Systems
- Routable communications between EACMS and PACS associated with High Impact BES Cyber Systems
- ESP(s) associated with Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCAs
- Routable communications between EACMS (either internal or external to the ESP) associated with Medium Impact BES Cyber Systems with External Routable Connectivity
- Routable communications between EACMS and PACS associated with Medium Impact BES Cyber Systems with External Routable Connectivity

CIP-networked environment is inclusive of CIP devices (BCS, EACMS, PACS and PCAs) only.
CIP-networked environment is inclusive of communications between a PACS and EACMS. Communications between a PACS and any other device is out of scope.

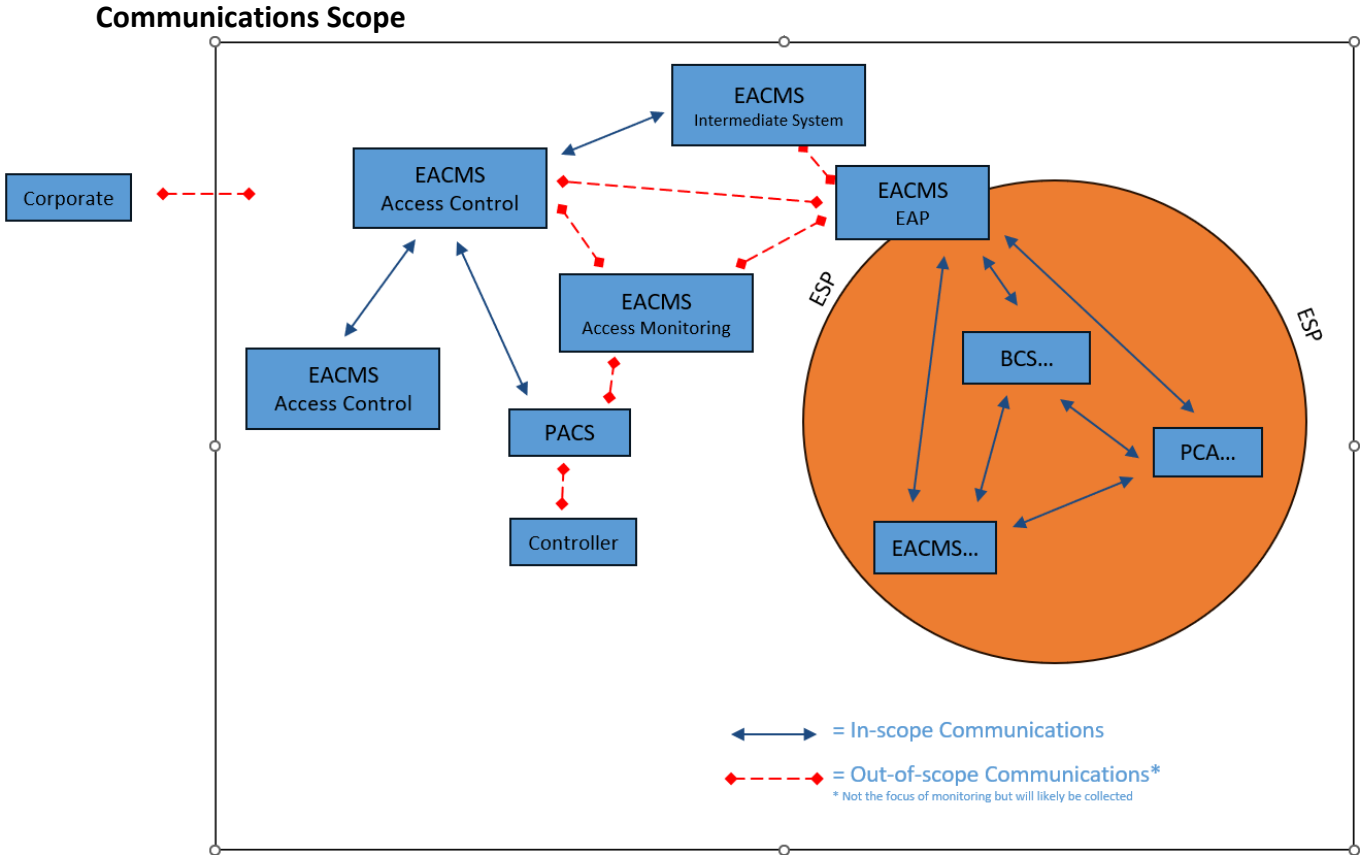



*Figure 1*

The SDT included these communications within the scope of the INSM Requirement R6 applicable systems.

### *Rationale for INSM Monitoring of associated EACMS, PACS, and PCA*

NSM, as described in Richard Bejtlich's book, The Practice of Network Security Monitoring, is most effective when collection occurs at strategic network locations and utilizes a variety of methods. "Network locations" is to be understood as a logical concept, rather than only being a physical locale within geographic space. Various devices perform technical functions within and between networks, such as switches, routers, and firewalls. These devices establish logical communication convergence points, which are ideal INSM collection points. Within the CIP framework, such devices are often classified as EAPs or EACMS. To most effectively monitor BCS network traffic, EAPs and EACMs must be considered. Methods for accessing network traffic include appliances, such as physical network taps; as well as logical configuration of network devices, such as port mirroring and network flow technologies.

Monitoring authentication traffic of SIEM or PACS management system is one way to detect many attack tactics; such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The SDT acknowledges that many entities already have significant capability to detect these tactics using existing systems, such as SIEM and EDR. Adding INSM monitoring will increase the level of assurance of these important systems and may contribute to detection and incident response capabilities.

The EACMS and PACS collection scope is limited.

- This scope does not require that INSM collection be installed between a PACS system and badge readers or panels or other PACS system components.
- This scope does not require INSM collection within components of an EACMS such as intra-directory traffic or intra-SIEM traffic.

## Rationale for Requirement R6 Part 6.1

*Requirement R6, Part 6.1: "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."*

### Background

The SDT attempted to write very specific collection requirements, but found that it would be untenable to write regulations that would properly address collection technology for all existing scenarios and technologies. Instead, the SDT proposed that responsible entities would design an INSM collection system that provides necessary data to meet Requirement R6, Parts 6.2-6.7. Requirement R6, Part 6.1 is to be a design or architecture of the INSM system. Requirement R6, Part 6.1 allows responsible entities wide latitude to design and implement an INSM data collection system that has the highest value in their network. A common first step in designing a collection system is to perform an assessment of the in-scope network using an assessment methodology.

**Assessment**

There are many methodologies that could be used as a guide to analyze networks to design an effective data collection system. Legitimate methodologies have originated from physical security, engineering, military, and cybersecurity. A few of these are listed in the following table:

| Name | Reference |
|---|---|
| **Mitre Attack** | https://attack.mitre.org/ |
| **Consequence-driven Cyber-informed Engineering** | https://inl.gov/cce/ |
| **Crown Jewel Analysis (CJA)** | https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis |
| **Proprietary Analysis methods** | Contact government partners or vendors |

The SDT recommends that the entity select any valid methodology and use the included processes to prioritize data collection to improve upon the existing visibility and detection capabilities of the organization.

Many important considerations exist when designing data collection for an INSM system. In allowing latitude in the design of an INSM system collection the SDT had two primary concerns:

1. That Regional Entities would require too much INSM collection and force entities to move resources from other effective cybersecurity detection systems such as SIEM and endpoint monitoring to INSM collection.
2. That responsible entities would not implement enough INSM collection to provide visibility of important network-based communications.

The following sections outline considerations to find a “just right” balance of INSM data collection that improves the detection capabilities of the entity.

### *Design*

The Design phase includes input from the network assessment and results in a description of where to deploy collection methods, which types of collection methods the responsible entity will utilize, and the data types to be collected.

The applicable environments for INSM collection have different network topologies, technologies, and support team capabilities. Collection environments differ and could include centralized environments such as control centers and generation or distributed environments such as substations. Collection technology could vary between transmission, distribution, generations, substations, renewables, and storage.

An additional consideration would be the network traffic. Control Centers may have relatively few industrial protocols (e.g., DNP3, ICCP, and Historian) with a large amount of software that is more “IT” in nature, such as databases, web services, and tiered application architectures. Substations might have no web services but a high percentage of industrial protocols such as IEC-61850, DNP3, SyncroPhasor, and

historian traffic. Variations in collection methods and tools are expected and warranted in an INSM system that provides balanced collection across various control systems.

### *Data Collection Methods*

The following table outlines some considerations for data collection from the SDT:

| Method | Comments |
|---|---|
| **Network TAPs (physical devices)** | Hardware costs are high.<br>Device failure scenarios are unknown to many vendors.<br>Deployment requires outages.<br>Can collect 100% of packets.<br>Good fit in centralized environments.<br>Collects layer 2 and layer 3 communications.<br>Usually not ERC. |
| **Port Mirrors/SPAN ports**<br>**Virtual Mirror ports (in a hypervisor)** | Little hardware required (although responsible entities will likely install network aggregators which have relatively high cost)<br>No outage required to enable.<br>Vendor experience and support varies.<br>Good fit in centralized environments.<br>Will increase processor utilization on layer 2 switches.<br>Packet loss (minimal amount) is expected.<br>Collects layer 2 and layer 3 communications.<br>Most SPAN ports pass data at layer 2 (not externally routable communications) and therefore, may not need to traverse an EAP.<br>Usually not ERC. |
| **Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)** | No hardware costs for forwarding.<br>Capable of performing in low bandwidth environments.<br>Good fit in distributed environments.<br>Good fit in low bandwidth environments.<br>Proprietary protocols vary per vendor.<br>Layer 2 collection capabilities differ by vendor.<br>Collects layer 3 communications.<br>Sampled NetFlow may be an option.<br>Can be generated by Switches, routers, and firewalls.<br>Probably requires ERC. |
| **RSPAN (remote SPAN)** | Collection is similar to Network Flow.<br>Requires higher bandwidth.<br>Can Collect layer 2 traffic.<br>Probably requires ERC. |
| **Sensor Deployment and management** | Usually requires TAPs or SPAN ports.<br>Most sensors require external data collection technology to gather data.<br>Hardware costs are high.<br>Relatively fast deployment in centralized environments.<br>High cost for distributed environments. |
| **SDN Networks** | Central management capability often built in. |

| | |
|---|---|
| | Can deny unauthorized traffic at layer 2.<br>Promising technology, but not widely deployed. |
| **"Bump in the Wire"** | Some systems, such as firewalls, have a capability of monitoring network data similar to TAPs. |
| **Endpoint Agents** | Some systems allow collection of network data using endpoint software. |

Thorough implementation of an INSM system often results in over-duplication of communications data. Individual packets are copied each time they pass another network monitoring location. Depending on the communications path, the number of monitoring points in the environment, and endpoints involved, a single Ethernet packet could be duplicated multiple times by the INSM system. This results in reduced resource efficiency and poor INSM system performance.

Some entities may decide to implement an INSM system utilizing fewer collection points located closer to the core of the network environments. In doing so, these entities may also implement technology to remove duplicated packets at or near the collection points prior to data being sent to the INSM system. Others may choose to deploy more INSM sensors closer to the end points on access layer switches. This reduces the amount of duplication, but increases the number of monitoring points. Either method, or a combination of the two, are acceptable. Classification of de-duplication appliances would likely be as a BCSI repository unless configured and classified differently by the Responsible Entity.

Deployment time for each technology is an important consideration to achieve compliance within the implementation timeframes of this requirement.

### *Out of Scope collection*

Requirement R6 does not require collection of data such as:

- Serial communications
- 4-20ma circuits
- Wide area network circuits such as MPLS (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used)

### *Relative/Generalized Implementation Timeframes of Collection Technology*

To attain compliance, a responsible entity will need to implement INSM within the necessary time frame. Implementation time will need to be considered. A very generalized table below outlines considerations of implementation timeframes after the entity completes product selection, planning, and testing of data collection components. The timeframes below do not account for delays caused by seasonal maintenance windows, inclement weather, disasters, and other operational considerations.

| | Control Centers | Generation Plants | Substations |
|---|---|---|---|
| **Network TAPs (physical devices)** | Months | Months | Years to Decades |
| **Port Mirrors/SPAN ports** | Months | Months | Months |
| **Network Flow** | Weeks | Weeks | Weeks |
| **RSPAN** | Weeks | Weeks | Depends on Bandwidth availability |
| **Sensor Deployment** | Months | Months | Years to Decades |

### *Data Collection Methods*

Part of the design considerations include specific plans of where to monitor the network, how to monitor each network collection point, and what data types will be gathered.

| Consideration | Example Options |
|---|---|
| **Identification of network collection points (Where to Monitor)** | Network Core<br>Network Distribution switches<br>Network Access layers<br>Carrier level (MPLS, etc.)<br>Identification of network convergence points |
| **Identification of Collection technology (How to Monitor)** | Network TAPs/Prisms<br>Mirror Ports/SPAN Ports<br>RSPAN configurations<br>Forwarding NetFlow data<br>SDN traffic logs<br>Other collection technology |
| **Identification of Data Types (Network Data Sources)** | Network Connection Creation<br>Network Traffic Content (PCAP)<br>Network Traffic Flow |

### *Principles and caveats*

As entities design a collection system by determining where, how, and which data sources are to be collected, regional entities and responsible entities should keep in mind several important principles and caveats related to achieving balance in INSM collection:

1. Requirement R6, Part 6.1 does not require data collection from every switch and every location on the network.
    a. As data is collected from more switches in a single broadcast domain, the amount of duplicate traffic will increase. Collecting the right data will sometimes require limiting collection points.

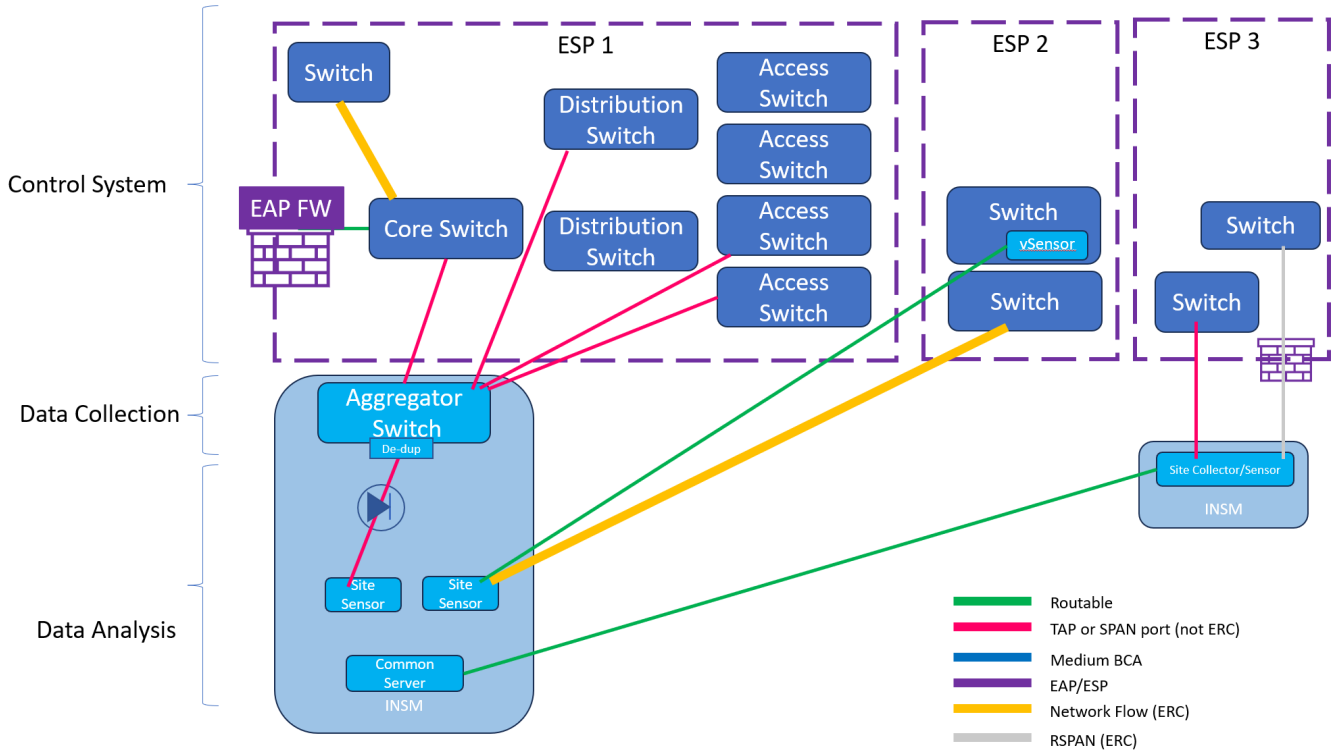
2. The entity might perform a threat assessment of adversary tactics, techniques, and procedures that have been used in attacks of other entities. This analysis might drive collection priorities to focus on targeted threats and threat vectors rather than broad collection of data with lower value.
3. A compliant low maturity INSM collection could focus on network locations and network source data that provide breadth of collection. Entities can then use this data to evaluate additional network collection points, collection technology, and data types that are needed to improve the system over time by adding or removing collection points and modifying collection methods.
4. Existing INSM products do not have the capability to identify or analyze all industrial protocols. When selecting tools to use for automated analysis, entities may choose to select data collection methods which align with the capabilities of tools and recommended by the tool vendors. Protocol identification errors do not constitute potential non-compliance.
5. Operational changes might require temporary or extended removal of INSM collection at some locations. In some situations, disabling collection or suppressing alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R6, Part 6.1.
6. Known and expected INSM limitations include:
    a. Limited analysis of encrypted traffic;
    b. High rates of false positive alerts;
    c. Wireless collection, especially in mesh networks, leads to inconsistent data collection; and
    d. Collection volume can frequently overwhelm existing analysis technology. There will exist situations when network volume reduces the visibility of network traffic. This is a known limitation of INSM technology and does not justify a potential non-compliance finding.
7. Centralized environments (control centers and generation) will likely require TAPs and/or SPAN ports to achieve balanced levels of visibility.
8. Distributed environments (substations) are more likely to deploy distributed collection, such as Network Flow or RSPAN. Entities may choose to deploy devices in distributed environments, or they may collect substation data from network aggregation points or optionally at larger substations to provide a balanced level of visibility.
9. Networks that connect to external private networks, such as turbine monitoring systems, ICCP connections, etc., are high value networks for INSM data collection and should be included in a balanced collection system.
10. Responsible entities that have mature endpoint collection and detection systems may not require as much INSM collection to achieve balanced collection, as an entity that does not collect detailed endpoint logs including memory and process logging. Existing breadth of detection can be visualized using tools such as MITRE Att&ck. Reports that demonstrate detection capability can be used to identify blind spots and to demonstrate balance.

11. An entity with mature firewall logging capabilities and extensive segmentation may choose to include firewall logs to augment INSM collection.
12. Some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a balanced approach might include a collection of firewall logs or logging communications at an upstream location rather than installing more hardware and reducing the overall reliability of the system. Alternatively, forwarding Network Flow data from routers or firewalls may be a more balanced method of collecting data.
13. Use of modern technology, such as Software Defined Networks (SDN), may provide relevant data as part of an INSM data collection system.
14. Collecting INSM data from multiple switches in a broadcast domain may result in significant data duplication. Entities may choose to collect data at locations that minimize redundant data collection (e.g., multicast and broadcast traffic) or to implement network aggregation tools that provide deduplication capabilities.
15. Filtering or elimination of traffic with low cybersecurity value (backups, replication, video, encrypted traffic, etc.) is expected in a balanced INSM collection system.

Balance in INSM collection and compliance with Requirement R6, Part 6.1 is achieved by having broad detection capability. As entities move through a maturity process, they may start with broad levels of network collection. As they mature detection capabilities, an entity that collects detailed data from endpoints and other systems may find that a reduction in network collection is justified. High maturity entities might use threat intelligence information to further refine and change data collection and focus detection efforts on tactics that have been observed and published through information sharing networks. At every level of maturity, the goal of INSM and other detection systems is to detect adversarial activity in networks and on endpoints. An entity that can demonstrate the ability to detect a broad array of adversary tactics and techniques using INSM and other systems is compliant with the intent of Requirement R6, Part 6.1.

### *Reference Architecture*

A sample reference architecture for INSM collection and logging data is shown below. This diagram is intended to show a wide variety of possible collection methods. Entities are not expected to implement all of these, but rather to choose and implement the collection methods that provide the most value to the entity.




This reference architecture has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.

- A network TAP or SPAN port sends data to a local data collection device.

**Emerging Technology**

The SDT acknowledges that this reference architecture does not properly represent all emerging and extremely promising technologies, such as software defined networking (SDN) and endpoint-based network isolation technologies. Entities that utilize SDN or similar technologies are encouraged to work with network vendors and detection vendors to design systems that will achieve the goals outlined in this document. SDN can provide network visibility and has the capability of preventing unauthorized network communications. Prevention capability afforded by SDN and other software-based tools is a significant step towards the goal of protecting the BES.

A properly implemented software-based detection and prevention solution may provide higher levels of protection than a passive INSM system. An entity that demonstrates a software-based solution which prevents attacks and logs the blocked network communications has met the intent of the Requirement R6, Parts 6.1 and 6.2 data collection and logging requirements. Additionally, software-defined policies that allow only authorized and expected communications explicitly meet, and exceed, the intent of Requirement R6, Part 6.3.

Technology which blocks unauthorized communication is deemed to meet the intent of Requirement R6, Parts 6.4 and 6.5 by both detecting that the communication is not authorized, and implementing a pre-defined action such as “block” or “learn.” An entity that shows example policies and the resulting network communications, as outlined above, has demonstrated compliance with these requirements.

## Rationale for Requirement R6, Part 6.2

*Requirement R6, Part 6.2: “Log collected data regarding network communications at the network locations identified in Part 6.1.”*

Collecting and logging network traffic is a core requirement of INSM (Requirement R6, Part 6.2).

### *Log*

When network traffic is collected, there are common ways to store the traffic logs for analysis including, but not limited to:

- Analyzing logs through a series of pattern searches, content rules, algorithms such as artificial intelligence or machine learning, storing relevant data and results, then discarding the actual network traffic.
- Forwarding log information to a searchable database for retention.
- Summarizing logs in a searchable database.

## Rationale for Requirement R6, Part 6.3

*Requirement R6, Part 6.3: "Evaluate the collected data to document the expected network communication baseline."*

In the context of INSM, the required network communication baseline is a record of past network communication and traffic. A baseline could include information about the traffic, such as:

- Layer 2 traffic, such as:
  - ARP;
  - ICMP;
  - DHCP requests;
  - Multicasts;
  - Broadcasts;
  - Source MAC addresses;
  - Destination MAC addresses;
  - VLAN tags; or
  - CDP/LLDP
- Layer 3 traffic, such as:
  - Source IP addresses;
  - Destination IP addresses;
  - Source TCP and UDP ports;
  - Destination TCP and UDP ports;
  - TCP header information; or
  - TCP payload metadata (size, content, determination if encrypted)
- Connection Creation information
  - TCP 3-way handshake; or
  - Connection termination information
- Summarizations of any of the above data
  - In control networks there are devices that send very repetitive data across the networks at high frequency. A summarization of this data is an acceptable part of baseline. For example, a turbine controller that continuously multicasts turbine status information at a rate of 100 multicasts per second is an example of communications that might make sense to summarize rather than to store in a raw format.
- Software and protocols in use on the network

- Some network communications can be linked to specific software with a high degree of confidence. Examples include telnet, ftp, dns, smtp, snmp, ICMP, and similar unencrypted protocols that have internet RFP standards defined. However, some network communications may require analysis to infer the software being used. It is understood that encrypted payloads using common tcp or udp ports may be difficult to identify correctly. INSM systems with accurate network communications protocol (software) classification are highly useful for cybersecurity investigations. Responsible entities are encouraged to use tools that classify the software being used, it is understood that no system will achieve 100% protocol identification accuracy.

➢ Asset information

- Network data may be used to gather information about assets communicating on the network which is useful for cybersecurity investigations. Entities are encouraged to use tools that identify assets and enrich asset data, it is understood that no system will achieve 100% accuracy of asset information from network analysis.

| 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 |

There are at least two justifiable purposes for maintaining this network baseline information:

1. Baseline data and network traffic is often used as a starting point when hunting for threat activity. An unusual traffic pattern or unexpected connection attempt might lead to expanded investigations through other log sources including endpoint logs, firewall logs, application logs, dns traffic, and other relevant data sources.
2. Cybersecurity analysts can search through the data to answer relevant questions related to cybersecurity investigations.

Baseline network traffic data is normally expected to be stored for an amount of time and then discarded. Depending on the type and amount of data retention, times could vary from seconds (for payload data – especially encrypted content) to several months for network connection and content summaries. Requirement R6, Part 6.3 does not include any expectation that the entity would manually create a list of all known good traffic and update that documentation at a regular interval. Instead, Requirement R6, Part 6.3 is an expectation that the entity can look at a history of actual traffic that can be used for further investigations, threat hunts, and incident response.

Note: as used here, the term *"baseline"* connotes a baseline of network traffic. This is distinct and separate from a baseline of configuration settings as used in CIP-010-4.

## Rationale for Requirement R6, Part 6.4

*Requirement R6, Part 6.4: "Deploy one or more method(s) to detect anomalous activities, including connections, devices, and network communications using data from Part 6.2."*

There are many methods that can be used to monitor logs to detect anomalous activity including, but not limited to:

- Threat Hunting
- Signature based alerts
- Correlation of signatures with other logged activities
- Anomaly Detection (as defined by a software tool or vendor)
- Artificial Intelligence and Machine Learning
- Other proprietary and open-source methods

Compliance with Requirement R6, Part 6.4 will probably result in many notifications. There is no expectation in Requirement R6, Part 6.4 that every notification generated by a tool requires human response. At the beginning of an INSM implementation, many notifications can be safely ignored. With time, maturity, and tuning, the entity will likely adjust the notifications in a way that balances false positive notifications with true positive notifications which require additional analysis (see Requirement R6, Part 6.5).

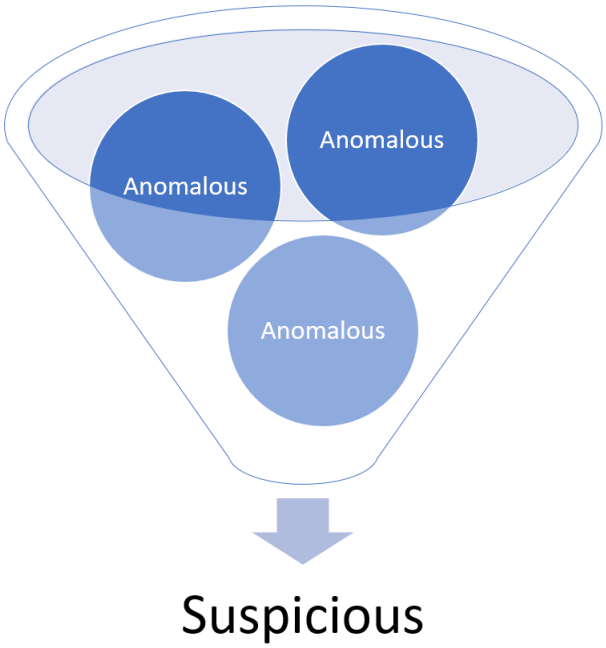
An entity may choose to comply with Requirement R6, Part 6.4 by logging all occurrences of specific events. For example, an entity may choose to alert on every connection using ssh and RDP with the knowledge that these alerts are nearly always authorized. By pre-generating events for these expected remote connections, an entity can visualize patterns that help detect unauthorized connections. These visualizations are useful during incident response investigations and threat hunting activities to help analysts differentiate between valid connections and suspicious connections. There is no justification for non-compliance with Requirement R6, Part 6.4 if entities automate generation of specific events. This is often an example of security automation and is an indicator of a proactive security process rather than a non-compliant organization.

**Terminology**

As used in this document and the INSM Requirement R6 and its part, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the entity might classify communications as benign, suspicious, or other similar classifications.

Unless specified, use of the word "anomalous" or "anomaly" in this document, does not refer to any proprietary technology commonly referred to as "anomaly detection."

The SDT debated using other terms and, at one point, used the term suspicious. After extended discussion and consultation with project observers, the term "anomalous" is used to indicate any notification or communication that is unexpected. As used in this document, "suspicious" is a term applied to network traffic or data after analysis has been performed on it resulting in escalation to a higher level of interest. Suspicious traffic may or may not require escalation to an incident response process, such as defined in Reliability Standard CIP-008.




It is expected that INSM systems will require constant and ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while alerts are being tuned to provide a higher signal to noise ratio.

## Rationale for Requirement R6, Part 6.5

*Requirement R6, Part 6.5: "One or more process(es) to evaluate anomalous activity identified in Part 6.4 to determine appropriate action."*

"The most important component of NSM is the analysis process. This is where the analyst takes the output from a detection mechanism (Requirement R6, Part 6.4) and accesses various data sources to collect information that can help them determine whether something detrimental to the network or the information stored on it has actually happened. The process the analyst goes through in order to accomplish this is called the analysis process." (Applied Network Security Monitoring Chapter 15)

When an organization first deploys INSM and begins analyzing the information generated by an INSM system, it would be normal and expected that the response and analysis process is ad-hoc. An ad-hoc process would meet the intent of Requirement R6, Part 6.5 for an entity without time and experience. As more time, experience, and maturity develops within an organization, the analysis process should necessarily improve from an ad-hoc state to a more formal process and procedure. Responsible entities may choose to adopt other existing analysis processes used for other cybersecurity tools, such as SIEM. A mature entity would have specific procedures, processes, playbooks, and automation to analyze anomalous network activity prior to escalation.

Compliance with Requirement R6, Part 6.5 requires some analysis be performed on the data as a starting point to detect malicious activity. This may be as simple as classifying the notification based on risk so that analysts can respond to high-risk notifications and not waste time with low-risk notifications.

An analysis methodology in a mature environment might include recurring threat hunts with hypothesis based on observed notifications or external threat intelligence.

The following are important points:

1. There is no specific response timeframe for every situation.
    a. If an entity is in the middle of investigating an active cybersecurity event and many high-risk notifications have occurred, it may be perfectly acceptable for the response team to triage high-risk or high-severity events into a "dumpster fire" category and ignore those events for hours or days while focused incident response activities occur.
2. During normal situations, it is expected that responsible entities would assess high-risk or high-severity notifications in a more-timely fashion

**Confidence Level**

Order No. 887 states that responsible entities have the capability to "identify anomalous activity to a high level of confidence." To achieve a high-level of confidence, responsible entities are expected to add INSM to existing detection systems and processes. INSM cannot replace other detection systems, such as SIEM or endpoint detection, but an entity might choose to add network communications information to a SIEM in order to meet the Requirement R6 and its parts, or an entity might include INSM data in an existing SIEM or similar tool.

An entity that has implemented a system that: (1) logs network traffic, (2) maintains logs and other data collected regarding network traffic, and (3) minimizes the likelihood of an attacker removing these logs, is deemed to have achieved this high level of confidence.

## Rationale for Requirement R6, Part 6.6

*Requirement R6, Part 6.6: "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."*

Requirement R6, Part 6.6 allows responsible entities to choose which data to store for longer periods of time while discarding data that is repetitive or has diminishing value over time. It is expected that retention will specify longer retention timeframes of data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time.

A sample retention chart is provided below to demonstrate retention considerations:

| Data Type | Cybersecurity Value over time | Retention Cost | Suggested Retention Timeframes |
|---|---|---|---|
| **Full PCAP (payloads)** | Value diminishes quickly with time<br><br>Encrypted payloads have little to no value | High | Commonly 0-3 days<br><br>Some use cases that could specify days to weeks or more if desired.<br><br>Some use cases could specify no collection or retention of payload data at all.<br><br>Retention is more likely to occur in centralized environments such as control centers and generation. |
| **Targeted PCAP (payloads) generated as part of an analysis or investigation.**<br><br>**Network traffic records generated as part of an analysis or investigation** | Value diminishes slowly with time | Low | If found to be evidence of a Cyber Security incident, then retention is specified by entity's CIP-008 process.<br><br>If no incident was found, then retention should be aligned with the entity's data retention schedule. |
| **Network Connection data generated from pcap**<br><br>**Network flow data**<br><br>**Network Connection Information** | Value diminishes slowly with time | Low | Commonly 3-6 months<br><br>Longer timeframes are acceptable per INSM system capability. |

- The SDT notes that many tools in 2023 commonly set retention at approximately three (3) months, which is an acceptable timeframe given the threat environment and tool capability in 2023. The SDT encourages vendors to increase retention capabilities of tools to match adversary dwell time.

In many INSM tools, data retention is specified by the number of events or records of network communications that can be stored. Network traffic spikes, which are common in applicable networks,

consume a larger volume of storage space. It is expected that retention timeframes specified are moving average targets rather than absolute date values.

As the maturity level of INSM systems increase, it is also expected that data collection may be filtered to exclude data that is deemed to be of lower value. For example, it is highly likely that an entity would choose to exclude backup traffic, video traffic, replication traffic, virtual machine migration traffic, and other high volume/low value data from collection. These exclusions enhance the ability of an INSM system to analyze traffic and generally result in higher signal to noise ratios and better detection outcomes.

## Rationale for Requirement R6, Part 6.7

*Requirement R6, Part 6.7: "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."*

A common adversary tactic is "Indicator Removal." The intent of Requirement R6, Part 6.7 is to protect the collected INSM data from modification or deletion by an adversary.

Suggestions for compliance with this requirement include controls used to protect BCSI and EACMS system. Some additional suggestions that should be considered to safeguard INSM data include:

- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Granting only authorized personnel access to the INSM system.
- Segmentation of the INSM system into an isolated network separate from OT and corporate networks.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Note that no part of Requirement R6, Part 6.7 is intended to limit information sharing with partner utilities, government partners, and other cyber security intelligence partners. The focus of Requirement R6, Part 6.7 is to ensure the data is available and has integrity.