A. Introduction

1. **Title:** Cyber Security – Internal Network Security Monitoring

2. **Number:** CIP-015-1

3. **Purpose:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1 Distribution Provider: One or more of the following Facilities, systems, and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1 Each UFLS or UVLS System that:

4.2.1.1.1 is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2 performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2 Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3 Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2 Responsible Entities listed in 4.1 other than Distribution Providers: All BES Facilities.

4.2.3 Exemptions: The following are exempt from Reliability Standard CIP-015-1:

4.2.3.1 Cyber Systems at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2 Cyber Systems associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESP).

4.2.3.3 Cyber Systems, associated with communication networks and data communication links, between the Cyber Systems providing confidentiality and integrity of an ESP that extends to one or more geographic locations.

4.2.3.4 The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.5 For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.6 Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact with External Routable Connectivity (ERC) according to the identification and categorization processes required by CIP-002 or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for CIP-015-1.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity. The documented process(es) shall include each of the following requirement Parts: *[Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment]*

1.1. Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications.

1.2. Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1.

1.3. Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s).

M1. Evidence must include each of the documented process(es) that collectively include each of the requirement Parts in Requirement R1 and evidence to demonstrate implementation of the process(es). Examples of evidence of implementation of the requirement Parts may include, but is not limited to:

Part 1.1.

- Documentation detailing network data feed(s) that includes a documented risk-based rationale that describes how network data feed(s) were selected for data collection.

Part 1.2.

- Documentation of anomalous network detection events;
- Documentation of configuration settings of internal network security monitoring systems;
- Documentation of network communication baseline used to detect anomalous network activity; or
- Documentation of other methods used to detect anomalous network activity.

Part 1.3.

- Documentation of method(s) used to evaluate anomalous activity;
- Documentation of actions in response to detected anomalies; or
- Documentation of escalation process(es) that could include CIP-008 Cyber Security Incident response plan(s).

R2. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity at a minimum until the action is complete in support of Requirement R1, Part 1.3. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

M2. Examples of evidence may include, but are not limited to, documentation of the internal network security monitoring data retention process(es), system configuration(s), or system-generated report(s) showing data retention with timelines sufficient to support Requirement R1, Part 1.3.

R3. Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification. *[Violation Risk Factor: Lower] [Time Horizon: Same Day Operations and Operations Assessment]*

M3. Evidence may include, but is not limited to, documentation demonstrating how internal network security monitoring data is being protected from the risk of unauthorized deletion or modification.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records, and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity did not implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications. (1.1.). OR The Responsible Entity did not implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1 (1.2.). OR The Responsible Entity did not implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s) (1.3.).	The Responsible Entity did not include any of the applicable requirement Parts for detecting and evaluating anomalous network activity.
R2.	N/A	N/A	N/A	The Responsible Entity did not implement, except during CIP Exceptional Circumstances, one or more documented

				process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Part 1.3.
R3.	N/A	N/A	N/A	The Responsible Entity did not, except during CIP Exceptional Circumstances, implement one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	5/9/2024	Approved by the NERC Board of Trustees.	