NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

FAQ for Reliability Standard CIP-015-1

April ~~5~~24, 2024

CIP-015 – Internal Network Security Monitoring

Q – What is internal network security monitoring (INSM)?

INSM refers to a forensic cyber security technology where entities copy network traffic in a trusted network zone, like an Electronic Security Perimeter (ESP), and ~~redirect~~ feed that copied network data to an INSM system that is capable of establishing a pattern of expected network traffic. FERC calls this pattern of expected network traffic a "baseline" in Order No. 887.[1] Once the expected network traffic baseline has been established, subsequent incoming network traffic is compared against the baseline and traffic that does not match the baseline in the INSM system is detected as anomalous and alerted on. These detections require analysis to determine if the anomalous network traffic is normal and benign, abnormal but not suspicious, or potentially malicious. FERC Order No. 887 states that, "INSM consists of three basic phases: (1) collection; (2) detection; and (3) analysis.[2] Taken together, these three stages provide the benefit for early detection and alerting of intrusions and malicious activity."[3]

Q – How is INSM different from traditional intrusion detection systems (IDS)?

Traditional IDS systems are categorized as performing signature-based detection of malicious activities. Similar to traditional anti-virus systems, IDS relies on an understanding of known malicious computer code for detection of malicious activity in a network. Duplicated network traffic ~~sent~~ fed to an IDS is then compared directly against the known signatures of malicious code implemented in the IDS. If the network traffic matches one of the signatures, an alert is issued. INSM does not typically use signatures of known malicious code. Instead, INSM relies on developing a pattern of expected network traffic and then compares incoming traffic against that pattern to identify potentially malicious traffic.

Additionally, IDS systems do not typically store the network traffic fed to them for further analysis. Network traffic data is usually discarded once the signature comparison takes place. On the other hand, INSM systems are typically capable of storing the network traffic and other metadata associated with the anomalous detection for further analysis and threat hunting while deleting non-anomalous network traffic to reduce storage requirements.

---

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

[2] Order No. 887 at P 9.

[3] *Id.* (citing Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020), https://www.isaca.org/resources/news-andtrends/isaca-now-blog/2020/applied-collection-framework).

Q – What are the benefits of installing an INSM system?

FERC Order No. 887 paragraphs 10-12 describe the benefits as follow:

> *"The benefits of INSM can be understood by first describing the way attackers commonly compromise targets. Attackers typically follow a systematic process of planning and execution to increase the likelihood of a successful compromise. This process includes reconnaissance (e.g., information gathering), choice of attack type and method of delivery (e.g., malware delivered through a phishing campaign), taking control of the entity's systems, and carrying out the attack (e.g., exfiltration of project files, administrator credentials, and employee personal identifiable information). Thus, successful cyberattacks require the attacker to: (1) gain access to a target system; and (2) execute commands while in that system.*
>
> *INSM could better position an entity to detect malicious activity that has circumvented perimeter controls and gained access to the target system. Because an attacker that moves among devices internal to a trust zone must use network pathways and required protocols to send malicious communications, INSM will potentially alert an entity of the attack and improve the entity's ability to stop the attack at its early phases.*
>
> *By providing visibility of network traffic that may only traverse internally within a trust zone, INSM can warn entities of an attack in progress. For example, properly placed, configured, and tuned INSM capabilities such as intrusion detection system and intrusion prevention system sensors could detect and/or block malicious activity early and alert an entity of the compromise. INSM can also be used to record network traffic for analysis, providing a baseline that an entity can use to better detect malicious activity. Establishing baseline network traffic allows entities to define what is and is not normal expected network activity and determine whether observed anomalous activity warrants further investigation. The recorded network traffic can also be retained to facilitate timely recovery and/or perform a thorough post-incident analysis of malicious activity."*[4]

[4] *Id.* PP 10-12.

Q – Why did the Drafting Team (DT) choose not to create a NERC Glossary of Terms for "anomalous"?

The DT considered whether or not to create a NERC Glossary of Terms entry for "anomalous". After reviewing the Merriam-Webster dictionary definition, the DT determined "anomalous" adequately described what is required in proposed Reliability Standard CIP-015-1, and it was not necessary to define the term in the NERC Glossary of Terms.

> "Anomalous - adjective
>
> 1: inconsistent with or deviating from what is usual, normal, or expected: IRREGULAR, UNUSUAL
> Example – Researchers could not explain the anomalous test results.
>
> 2 a: of uncertain nature or classification
>
> b: marked by incongruity or contradiction: PARADOXICAL[2]

Network anomaly detection is a well-known cyber security technique that provides network security threat detection. These systems track critical network characteristics in Real-time and generate an alarm if a strange event or trend is detected that could indicate the presence of a threat. Examples of such characteristics include excessive traffic volume, excessive bandwidth usage, or unusual protocol use. The DT determined that this technology has existed for many years, and it was unnecessary to define the term for industry. Many electric industry entities have already implemented, or are in the process of implementing, network anomaly detection solutions at their facilities. An additional reason for not defining the term is that "anomaly detection" is a phrase used by vendors to describe their proprietary technologies. However, in general, all vendors in the anomaly detection space compare incoming network traffic feeds against a baseline of known expected and normal traffic to detect something that is out of the ordinary, unusual, or unexpected. In a word: anomalous.

Q – Is network traffic required to be captured for Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs)?

The DT focused proposed Reliability Standard CIP-015-1, Requirement R1, on networks protected by an ESP. EACMS and PACS not protected by an entity's defined ESP are outside the scope of Project 2023-03 INSM. One example of EACMS and PACS Cyber Assets that are out of scope of Project 2023-03 INSM would be those existing in a demilitarized zone (DMZ) not protected by the entity's BES Cyber System's ESP(s).

Entities that choose to protect EACMS, PACS, and PCAs with a defined ESP should consider network traffic from those systems to be in scope for proposed Reliability Standard CIP-015-1, Requirement R1. Protected ESP networks connected to EACMS, PACS, and PCAs should be considered for data collection and monitoring for anomalous network traffic, as these systems are not immune from attempts to compromise, and they could serve as pivot points for an attack on a Bulk Electric System (BES) Cyber System protected by the same ESP.

[2] https://www.merriam-webster.com/dictionary/anomalous

Q – What does the DT mean by "network activity"?

In Order No. 887, FERC directed NERC to develop standards to address the need for Responsible Entities to monitor for and detect unauthorized activity, connections, devices, and software. The DT intends for the term "network activity" to represent the connections between devices and software included in the network traffic that an entity is collecting as it passes between hosts that are protected by an ESP.

Q – How should an entity decide which ESP networks to monitor and set up data feeds?

Entities are expected to identify which networks are protected by an ESP and use a risk-based rationale to determine where data feeds should be implemented to provide the best opportunities for detection of malicious activity, as set forth in ~~-~~proposed Reliability Standard CIP-015-1, Requirement R1, Part ~~R~~1.1. Entities should document their risk-based rationale for assessing which networks to monitor in their INSM process.

For example, entities may choose not to collect data from networks that only carry backup traffic because workstations and servers do not typically route their normal traffic across that backup network. Otherwise, an entity would likely have to capture and temporarily store tremendous amounts of non-malicious backup traffic. From a risk-based perspective, backup networks pose limited risk and would likely not be a good use case for INSM. Likewise, monitoring of encrypted connections provides limited INSM value because all of the traffic passing on that network connection is encrypted, and INSM would be unable to decrypt and analyze the encrypted packets. An entity will realize more cyber security value, from an INSM perspective, if they monitor the decrypted traffic on the other ports on that switch where the VPN tunnel is connected. Entities need to document these kinds of evaluations of an entity's network as evidence for proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1.

A few examples of high-risk networks that should be given extra consideration for providing data feeds would include network traffic associated with an entity's energy management system (EMS) or distributed control system (DCS) server(s) and workstations, third-party connections, traffic associated with authentication servers (e.g., Active Directory or two-actor authentication systems~~)~~, and programmable logic controller (PLC)/remote terminal units (RTU) communication paths~~)~~. Each entity's ESP networks will be unique to that entity; therefore, the DT has left it up to the entity to make risk-based decisions, like those described, to determine what network traffic data feeds should be collected to provide the entity's INSM system with the best opportunity for detecting malicious traffic that could be indicative of an attack in progress.

Q – What is the difference between monitoring in CIP-005-7, CIP-007-6, and CIP-015-1?

Reliability Standard CIP-005-7 is exclusively concerned with the monitoring of ESPs. Reliability Standard CIP-005-7, Requirement R1, Part 1.5 requires entities to monitor at the ESP's Electronic Access Point, "For detecting known or suspected malicious communications for inbound and outbound communications." By specifying "known or suspected malicious traffic," it implies the use of signature-based detection methods for known malicious code. Requirement R1, Part 1.5 does not require monitoring of any traffic that is only passing between Cyber Assets within a defined ESP and is focused on traffic passing through the EAP.

FERC Order No. 887 aims to address this gap in cyber security monitoring by requiring INSM implementation.

Reliability Standard CIP-007-6, Requirement R3, Part 3.1 is focused on implementation of traditional signature-based technologies, such as anti-virus, on Cyber Assets. As noted above, this lack of a requirement for monitoring network traffic in the ESP represents a gap, as entities previously were not required to inspect internal ESP traffic for malicious activity.

While Reliability Standard CIP-007-6, Requirement R4, does allow logging of events at the BES Cyber System level, the DT would contend that most entities are meeting this requirement by logging events at the Cyber Asset level in a security information and event management (SIEM) system. The SIEM may also be used for analysis and retention of those host level events to meet Reliability Standard CIP-007-6, Requirement R4, and allow for detection of login attempts and malicious code on those Cyber Assets themselves. INSM would likely be unable to determine whether a login attempt failed or definitively detect malicious code installed on a Cyber Asset and is not a suitable technology to meet Reliability Standard CIP-007-6, Requirement R4, Part 4.1.

Proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.1. will require entities to implement the method(s) of their choice to ~~copy~~ feed the network traffic the entity identified for capture in a defined ESP to a system that can identify patterns of expected network behavior. For proposed Requirement R1 Part 1.2, the INSM detects network traffic from the data feeds that is anomalous based on a comparison with the INSM system's patterns of expected network behavior. Network data associated with an anomalous detection should be protected and retained at least until the required evaluation can be completed in proposed Requirement R1, Part 1.3. The detection should be evaluated and triaged appropriately in proposed Requirement R1, Part 1.3. The DT considers proposed Reliability Standard CIP-015-1 to be an additional cyber security control that can increase the probability of detecting malicious activity in networks protected by an ESP.

Q – What data are entities required to retain and for how long?

Proposed Requirement ~~R3~~ R2 requires an INSM system to be able to store network traffic data and other metadata associated with each detection of anomalous activity. Data associated with non-anomalous traffic is not required to be retained. Most modern INSM systems are capable of saving just the data associated with anomalous network activity and discarding the rest.

Network and metadata associated with anomalous network activity must be available for the evaluation conducted in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Network and other data associated with false positives and other detections deemed by the entity not to be malicious do not need to be further retained after they have been evaluated in proposed Requirement R1, Part 1.3. However, data associated with potential attempts to compromise, or a suspected cyber security event, should be retained and fed into the entity's Reliability Standard CIP-008 incident response process(es) for further investigation. **Note:** Reliability Standard CIP-008 has its own retention requirements that entities need to keep in mind as they develop their proposed Reliability Standard CIP-015-1 retention process(es).

Q – How does the DT intend for entities to protect INSM data?

FERC Order No. 887 directed NERC to implement measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. In DT discussions it was clear that the intent was to protect the anomalous network data collected from being tampered with or removed by an adversary such that an entity could not accurately complete the required evaluation in proposed Reliability Standard CIP-015-1, Requirement R1, Part 1.3. Malicious actors typically attempt to hide their tracks by removing evidence on a host system. Because network traffic captured in transit between hosts cannot typically be modified by an attacker, it is that data which entities need to protect. This provides an entity with evidence that, if its integrity is maintained, can serve as a true source of what is happening on a network.

Entities must protect their INSM data from unauthorized deletion or modification in support of proposed Requirements R1 and ~~R3~~R2. Typically, this is done through the use of cyber and physical security controls. Entities should restrict electronic access to the INSM system and INSM data to only those with a need to access it. Restricting physical access to the INSM system is another good control. Use network segmentation to ensure that the INSM system is not part of the same networks the INSM system is monitoring. File integrity monitoring is another option to consider. Entities have developed a range of controls, and the controls they implement should be in line with their existing information protection programs.

Entities will need to assess the data being collected, and the meta data created by an INSM system, to determine if it needs to be protected as BES Cyber System Information (BCSI). Entities that declare the information stored in their INSM system as BCSI and protect the INSM data with their BCSI information protection procedures developed for Reliability Standard CIP-011-2, should meet proposed Reliability Standard CIP-015-1, Requirement ~~R2~~R3. If an entity decides that the information is not BCSI, they must apply and document the security protections employed to protect the INSM data from modification or deletion.

Q – Why did the DT not include language that would allow a Technical Feasibility Exception (TFE) in situations where an entity believes they cannot implement INSM?

The DT determined that INSM should be capable of being installed, at least in some fashion, in any of an entity's ESP networks. INSM technologies have been developed specifically to be installed in operational technology (OT) environments as a passive detection mechanism and detect anomalous behavior in most modern OT protocols. Duplication of network traffic can be accomplished through the use of hardware network taps, which were invented in 2000, or switch port mirroring (Cisco calls this SPAN) available on commercial and industrial network switches for over the past 10 years.

Q – Is CIP-015-1 cost-effective?

In consideration of the cost effectiveness of proposed Reliability Standard CIP-015-1, the DT provided flexibility to entities to design their INSM systems to meet the proposed Reliability Standard CIP-015-1 requirements no matter the configuration of the individual networks protected by ESPs. Modern control center/data center environments should be capable of replicating an ESP's network traffic. Virtualized

systems should have the capability to replicate internal traffic between Virtual Cyber Assets to an INSM system. Replacing a switch or substation network device to replicate network traffic at key network convergence points is typically an inconsequential expense for an entity. The DT concluded that the main expense will most likely be procurement of INSM software and/or hardware, installation, labor ~~count and~~ cost, and tuning the system prior to the proposed Reliability Standard CIP-015-1 enforcement date.

The DT provided an implementation timeframe of 36 months for high impact and medium impact with External Routable Connectivity (ERC) control centers to acquire, install, and tune their INSM systems. An additional 24 months, for a total of 60 months, was provided for the high impact and medium impact BES Cyber Systems with ERC in non-control center environments to become compliant with proposed Reliability Standard CIP-015-1. The additional 24 months were provided for entities to plan, budget, and acquire the necessary capability to detect anomalous network activity at those substation locations which may be more challenging to implement.

Lastly, the DT would remind entities that FERC issued Order No. 893[3] in 2023, which provides *Incentives for Advanced Cyber security Investment*. FERC Order No. 893 establishes rules for incentive-based rate treatment for certain voluntary cyber security investments by utilities. Implementing INSM prior to the enforcement date of NERC INSM standards was described in the FERC Order No. 893 as pre-qualifying. The DT cannot say whether a particular entity may or may not qualify for these incentives, but it is an option which entities may want to consider.

Q – Do entities have to capture traffic for serial connections?

As stated in the Technical Rationale, proposed Requirement R1 does not require collection of data such as serial communications, 4-20 ma circuits, or wide area network circuits such as multiprotocol label switching (MPLS) and other similar technologies.

[3] *Incentives for Advanced Cyber security Investment,* Order No. 893, 183 FERC ¶ 61,033, *order on reh'g,* Order No 893-A, 184 FERC ¶ 61.053 (2023); *see* e.g., FERC Cyber security Incentives web page - https://www.ferc.gov/cybersecurity-incentives