The Lighthouse

By Lew Folkerth, Principal Reliability Consultant, External Affairs

Preparing for Internal Network Security Monitoring (INSM)

What is INSM?

Internal Network Security Monitoring, or INSM, is the practice of understanding what is going on inside your networks. For the purposes of the CIP Standards, that means understanding what network traffic is occurring within your Electronic Security Perimeters (ESPs).

Today's CIP Standards only require monitoring of traffic into and out of an ESP. INSM is different in that it is monitoring of traffic within an ESP or other network.

Why is INSM important?

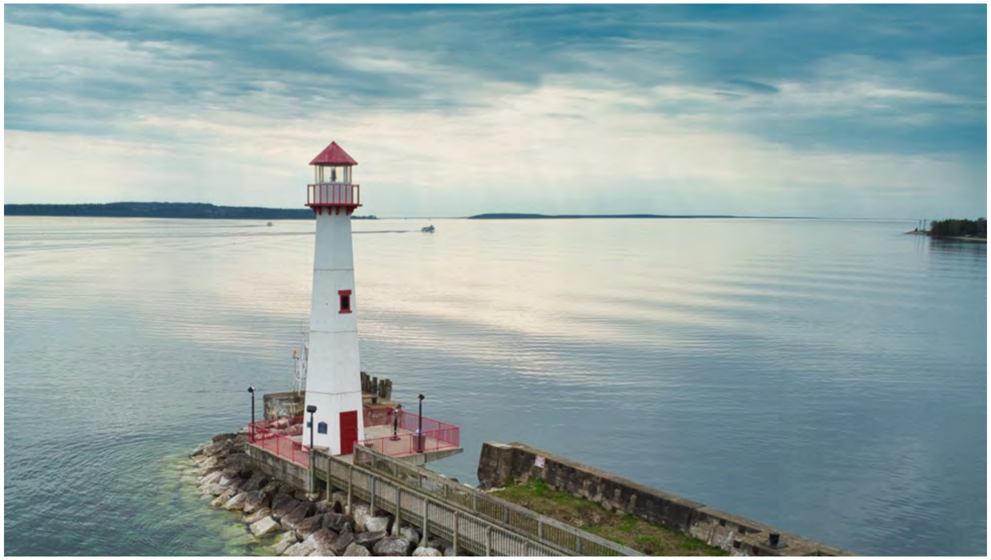
INSM addresses the risk of a malicious actor bypassing your ESP firewall and gaining network access to your ESP. Some malicious actors can evade detection by signature-based defenses such as antivirus solutions or intrusion detection systems.

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity. It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs. There are times that I also may discuss areas of the Standards that other Entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

In that case, there may be no way to detect that presence in your network without INSM. To address this risk, FERC issued Order 887.

Order 887

On January 19, 2023, FERC issued [*Order 887, Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*]. FERC directed NERC to "develop new or modified CIP Reliability Standards requiring INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress." [Order 887 at P3]



Wawatam Light, St. Ignace, Michigan – Photo: Lew Folkerth

NERC is required to ensure revisions to the CIP Standards achieve the following security objectives [paraphrased from Order 887 at P79-80]:

1. Develop a baseline for network traffic by analyzing network traffic and data flows for security purposes.
2. Monitor for and detect unauthorized activity, connections, devices, network communication protocols, and software inside the CIP-networked environment, as well as encompass

Continued on page 10

Continued from page 9

awareness of protocols used in industrial control systems.

3. Methods to ensure:
   a. logging of network traffic,
   b. maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation, and
   c. maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures.

Note that INSM is an industry security practice, while Order 887 calls for implementing INSM via revised CIP Standards.

What is the timeline for Order 887?

NERC is required to file the INSM revisions in mid-2024, so it's reasonable to expect an Effective Date for any new or revised Standards to be sometime in 2027. This estimated date will be influenced by many factors, so please don't hold me to this.

What preparation will be needed for INSM?

INSM is not a project where you can just buy some gear, install it, and be done. INSM will require getting extremely familiar with your Cyber Assets, the software they run, the protocols they use to communicate with other assets, and how the communications data flows under different conditions. Here are some things to consider when beginning your INSM journey:

Staffing – Entities large enough to have high or medium impact BES Cyber Systems will almost certainly need additional staff to implement INSM. Your staff will need to understand your operational environment, so just re-assigning IT staff may not be sufficient.

Training – Operational environments have specialized needs and require specialized skillsets. You will probably need to provide training for your operational security personnel, beyond that of typical IT training. Such training could be provided by vendors, by independent training organizations, or by your own specialists. The specialized skills needed will include understanding of the protocols being used within your networks and how those protocols are used by your equipment and processes.

Also see the article, "Cultivating a Talented and Engaged Workforce," in this Newsletter.

Initial monitoring points – You will need visibility into your applicable networks in order to begin developing your baselines. This will require carefully selecting one or more points in your network to begin monitoring. These initial points could be in a test or development network rather than in a production network.

Initial baseline – You will need to understand all the protocols in use and what those protocols are used for. Start small and begin working to build your network understanding and visibility.

Baseline minimization – You may want to consider ways to reduce the amount and types of traffic on your ESP networks. If possible, replace systems that generate unnecessary traffic with systems whose traffic you can tightly control.

Network segmentation – You may want to consider employing VLANs within your applicable networks to create multiple network segments with less traffic per segment. This can make your monitoring tasks easier by focusing on a smaller set of traffic per VLAN segment. Also, unauthorized traffic may stand out better if there is less traffic on the segment.

Continued on page 11

The Lighthouse

Continued from page 10

Monitoring strategy – As you gain a deeper understanding of your internal networks, you can develop or improve your monitoring strategy. Will you use network switch span ports? Will you use ethernet taps to create a shadow network for monitoring? Other techniques? Or a combination of techniques? Consider looking at other types of security programs within your entity, such as insider threat management.

Storage planning – You will need to store your monitoring data such as the retained logs or traffic captures. This data has the potential to be very large, so begin planning for that storage now. Since we don't yet know how long this data will be required to be stored, assume a substantial period of time such as a year. Due to the potentially large size of the data to be stored, you may want to consider a separate storage system for INSM data.

Information protection – After the information is gathered and stored, its confidentiality, integrity and availability will need to be protected. Include these plans in your overall strategy.

When should my entity start preparing for INSM and Order 887?

INSM is a detective control you can implement on any network, although it is especially valuable on sensitive networks such as ESPs. As such, it is a good idea to begin implementing INSM as a "best practice" security control without waiting for the revised standards to become effective.

While I expect the Effective Date for the Standards resulting from Order 887 could be in 2027, I strongly encourage you to begin your preparations now. You should identify your staffing and training needs and start addressing those needs. Don't wait until FERC approves the new requirements. Take advantage of the lead time being offered by the FERC Order and begin developing your staff, your baselines, and your monitoring strategies now.

References

- Order 887
- CMEP Practice Guide – Network Monitoring Sensors
- Project 2023-03 INSM Standard Development Page

Participate!

You have many ways you can participate in the standards development effort. You can volunteer for the drafting team. You can attend drafting team meetings. You can assist your entity in writing comments on the revised standards. You can influence your entity's vote on the revised standards. You can do any or all of these, but please get involved!

Requests for assistance

If you are an entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here.

Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, can be reached here.

Continued on page 10