SANS | Research Program

Buyer's Guide

NERC CIP-015: Monitoring Deep Inside Critical Networks to Keep Adversaries Outside

Written by **Tim Conway**
January 2025

DRAGOS

INSM Call to Action and CIP-015

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards (hereinafter referred to as the Standards) require preventive controls to establish Electronic Security Perimeters (ESPs) containing Bulk Electric System (BES) Cyber Systems and to control communications in and out of those ESPs.[1] In addition, the Standards require preventive and detective controls on the BES Cyber Systems directly. However, in light of demonstrated adversarial techniques to evade detection and maintain a persistence within operational networks, the Federal Energy Regulatory Commission (FERC) determined that additional detective requirements were necessary. Specifically, FERC directed that the new or modified standards needed to address the following security objectives:

- Establish baselines of internal operational network traffic.
- Monitor and detect unauthorized activity within the internal operational network.
- Log network traffic and maintain it in such a manner that minimizes the likelihood of an attacker destroying or modifying the traffic.

This FERC-directed action adds the necessity for east–west traffic monitoring (within the protected network from asset to asset) within CIP critical networks moving beyond the existing preventive and detective controls that focus on communications moving north to south (into and out of a protected network) from an untrusted segment into the trusted environment and reaching an endpoint. Although these communications are currently subject to NERC CIP requirements, they are also potentially vulnerable to a targeted adversary attack that compromises an asset in the untrusted segment and then leverages the approved system-to-system communication to pivot onto an asset within the trusted environment. FERC Order 887[2] directs additional detective controls within the trusted environment to examine communications occurring east to west between BES Cyber Systems.

The approach identified within FERC Order 887 highlights the three stages of INSM: (1) collection, (2) detection, and (3) analysis. These three stages represent implementation and process challenges across organizational workforce development, network infrastructure capabilities, and solution deployment. Considering the scope of the coming CIP-015 effort, it is essential for organizations to understand the Standards development process and the FERC call to action.

How FERC Works with NERC

Industry first started the development of the voluntary CIP Standards in 2003 with an Urgent Action Request, but the Standards eventually moved from voluntary to mandatory and enforceable through the Energy Policy Act of 2005. The Standards development process still engages asset owners and operators as the primary authors of the requirement language and balloting process. However, Standards activity does not always begin with the entities; they can also be proposed and directed by FERC. In recent years, FERC has directed Standards changes and Standards development activities based on assessed risks to the reliability of the bulk power system.

Such was the case with FERC Order 887. The Notice of Proposed Rulemaking was originally released in January 2022 amidst the escalating concern about Russia's imminent invasion of Ukraine. After consideration of comments, the Final Order was released, effective April 10, 2023. With growing concerns of adversary latent living off the land (LotL) capabilities and the need for expanded detective controls, FERC directed the industry to create new or modified Standards to require Internal Network Security Monitoring (INSM).

[1] Throughout this paper, terms specifically defined by NERC use NERC's capitalization convention.

[2] "Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems," E-1 RM22-3-000, www.ferc.gov/media/e-1-rm22-3-000

The Approved Waiting Period

All Standards development activities suffer from regulatory lag. When a set of developed Standards receives final approval from FERC, the effective date issued typically ranges between 18 and 36 months after the FERC approval date. The whole process can sometimes take three to eight years before an entity is required to implement the requirements. For CIP-015-1, the implementation plan is staggered with a 36-month effective date for High and Medium Impact Control Centers with External Routable Connectivity (ERC) and a 60-month effective date for other Medium Impact sites with ERC. As shown in Figure 1, FERC first raised this concern about a cybersecurity gap in protection in January 2022. After consideration of comments, FERC issued a final order effective April 10, 2023, calling for NERC to submit new or modified Standards addressing INSM within 15 months. NERC assembled a drafting team from the electric sector that created the CIP-015-1[3] requirement language and achieved industry approval through a final ballot on April 30, 2024. The CIP-015-1 Standard further received NERC Board of Trustees approval on May 9, 2024, and was filed with FERC on June 24, 2024. On September 19, 2024, FERC proposed to approve CIP-015-1, but also directed NERC to further expand the scope of the requirements to include extending protections outside of the ESP to Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). CIP-015-1 will become mandatory and enforceable for High and Medium Impact Control Centers with ERC on the first day of the first calendar quarter that is 36 calendar months from the date that the Final Order is recorded in the Federal Register officially approving CIP-015-1.[4]

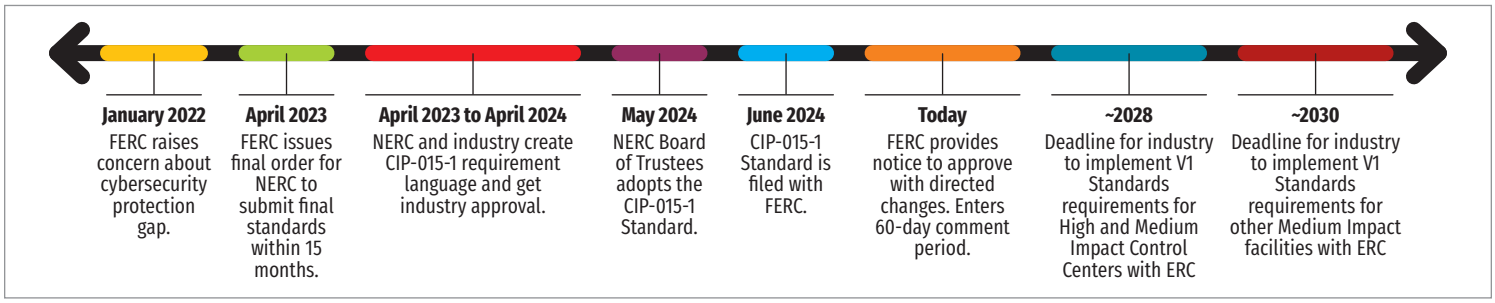

Figure 1. Evolution of FERC Order 887

The journey is long for many reasons, not the least of them being the transparent Standards development process, which allows for requirement development by industry for industry and considers open input from all stakeholders across the ecosystem. Additionally, the balloting process ensures that entities of various sizes, asset mix, entity types, and functional registrations receive a voice in crafting the potential requirements. After the requirements are approved, FERC also considers the capital projects and resources necessary to implement the requirements among the existing entity operating obligations. For this reason, organizations should remain engaged in Standards development activity to ensure they maintain a view on the requirements of the future. While some in the industry will need considerable time to secure budgets and resources and to begin their efforts to implement the requirements as the effective date draws closer, it is important to recognize there are actionable items within the CIP-015-1 set of requirements that should be pursued immediately.

While some in the industry will need considerable time to secure budgets and resources and to begin their efforts to implement the requirements as the effective date draws closer, it is important to recognize there are actionable items within the CIP-015 set of requirements that should be pursued immediately.

[3] "CIP-015-1 – Cyber Security – Internal Network Security Monitoring," www.nerc.com/pa/Stand/Reliability%20Standards/CIP-015-1.pdf

[4] "Implementation Plan: Project 2023-03 Internal Network Security Monitoring (INSM) Reliability Standard CIP-015-1," www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023-03%20Implementation%20Plan%20FB%20clean.pdf

The CIP-015-1 We Know Now

The currently filed version of CIP-015-1 contains a total of three requirements, with the first requirement containing three sub-requirements. The first requirement is responsive to FERC's Order, highlighting the stages of INSM, including collection, detection, and analysis. These highlights are captured in the Requirement 1 language that outlines how INSM activity is to occur within the entity ESP. It directly identifies each stage of INSM in each of the three sub-requirements:

1. **CIP-015-1 R1.1—**Implement, using a risk-based rationale, network data feed(s) to *monitor* network activity; including connections, devices, and network communications.
2. **CIP-015-1 R1.2—**Implement one or more method(s) to *detect* anomalous network activity using the network data feed(s) from Part 1.1.
3. **CIP-015-1 R1.3—**Implement one or more method(s) to *evaluate* anomalous network activity detected in Part 1.2 to determine further action(s).

Although each sub-requirement consists of a relatively short sentence, entities will quickly identify the performance impacts behind each word contained within the sub-requirement language and the associated level of effort to achieve the requirement at each High Impact and Medium Impact facility with ERC.

Requirement 1.1

Requirement 1.1 requires the identification of data feeds to monitor and provide the ability to defend the selection of specific feeds. This process will likely involve a diverse group of professionals who understand system-to-system data flows; operations personnel who understand real-time tasks that need to be performed and the systems necessary to perform them; as well as cybersecurity practitioners who can identify data feeds of interest based on adversary tactics, techniques, and procedures (TTPs). In addition, the data feeds chosen would need to support network activity monitoring activities that include connections, devices, and network communications. As entities review logical and physical network prints to identify appropriate collection points, they also must consider the existing network infrastructure and determine whether it and vendor agreements will support the necessary traffic collection. With a risk-based approach to selecting data feeds and a network infrastructure technically capable of collecting network activity, the entity also will need to ensure that connections, devices, and network communications all are being collected and monitored to satisfy strict compliance with Requirement 1.1. Although the identification of data feeds to collect is key to Requirement 1.1, note that targeted traffic capture and aggregation capabilities should be considered here as well. This is an important collection consideration that is informed by both the architecture and network infrastructure capabilities, as well as how the entity implements Requirement 1.2. (Without appropriate collection, detection will be deficient.)

Requirement 1.2

Requirement 1.2 requires asset owners and operators to be capable of leveraging all of the network activity collected in Requirement 1.1 and detecting any anomalous network activity within it. This requirement will move organizations into a maturity and capability model across their BES Cyber Systems, where they will need to establish baselines and have a full understanding of what normal network activity—as well its absence—looks like. Traditional IT detection rules may help identify untargeted malware or adversary activity, but Requirement 1.2 is looking beyond that and will require capabilities that provide Operational Technology (OT)-specific detections, behavior analytics, baseline deviations, and operational system models that can detect anomalous network activity patterns. As organizations pursue these capabilities, they will likely identify the need for new or expanded tools and solutions. This identification process introduces additional systems to secure and ensure compliance, in addition to expanded workforce training and processes to utilize the solution.

Requirement 1.3

Across the CIP standards, many requirements depend on each other for performance. To achieve Requirement 1.3, Requirements 1.1 and 1.2 must be in place and effective. After an entity has identified the necessary data feeds to collect and monitor from and has established a means to detect anomalous network activity, then Requirement 1.3 highlights the need to evaluate anomalous detections. The analysis phase of Requirement 1.3 demands the implementation of a process to:

- Evaluate detections for false positives.
- Include threat hunting capabilities to identify latent attacker actions.
- Inform future threat intelligence.
- Potentially intersect with the incident response and reporting requirements of CIP-008.

For consistency purposes, much of Requirement 1.3 will lean heavily on analysis processes or playbooks. For real-world LotL techniques, threat hunters will need to be knowledgeable and trained to understand the OT environment as well as attacker approaches to target a system. This blend of people, processes, and technology will be essential to demonstrate strict compliance with Requirement 1.3.

Although these three sub-requirements consist of only three short sentences, they represent a significant amount of work for CIP-affected entities throughout North America. The good news is that achieving the required level of INSM highlighted in the three sub-requirements also will require significantly more work for adversaries to maintain a latent persistence within the North American bulk power system critical networks.

Requirement 2

CIP-015-1 Requirement 2 is responsive to the FERC Order directive for "maintaining logs and other data collected regarding network traffic." In Requirement 2, the language specifies the need to retain INSM data associated with anomalous network activity. The Requirement 2 retention obligation is sandwiched between Requirement 1.2 and Requirement 1.3, meaning that entities only have to retain the data that has been determined to be anomalous in 1.2 and only for a duration necessary to support the analysis process of 1.3.

As organizations consider the solutions, processes, and workforce activity involved in performance of Requirements 1.2 and 1.3, they will naturally begin to identify data retention timing to support automated system detections as well as threat hunting and analysis activity. In addition, organizations will need to consider data retention capabilities required to support CIP-008 incident response retention obligations if the evaluation performed under CIP-015-1 Requirement 1.3 identifies anomalous traffic that is related to a Reportable Cyber Security Incident or a Cyber Security Incident.

Developing a benchmark of data rates, storage requirements, INSM performance timing, and analysis processes will take time as entity network activity data feeds, systems, and false positives are appropriately tuned.

Requirement 3

Requirement 3 addresses the FERC directive to minimize the likelihood of an attacker removing evidence to further evade detection or analysis. The requirement language is unique in that it does not pertain to only the Requirement 2 data related to network activities determined to be anomalous, which includes retention obligations. Requirement 3 also extends to Requirement 1 sub-requirements regarding monitoring, detection, and evaluation. Entities will need to consider the technology solutions and processes in place that mitigate the risks of unauthorized deletion or modification of the network activity data utilized in performance of the Requirement 1 sub-requirements.

Where Does Technology Fit?

When looking at technology and solution providers relevant to CIP-015-1, the first items to consider are technology and workforce pairing. The partnerships across solution providers and entities are key, especially in the areas of safety, reliability, cybersecurity, and compliance. Understand that none of these critical areas can be purchased. Instead, a culture must be created that intentionally pursues safety, reliability, cybersecurity, and compliance through specific work practices, training, and technologies that enable the workforce. Entities will need to consider the scope of their CIP universe, examine each of the CIP-015-1 requirements in Table 1, and then turn to solution providers to identify how they will shape their CIP program to satisfy the new requirements. As organizations evaluate the capabilities of the Dragos Platform and develop technical capabilities mappings, they will be pleasantly surprised with the technical feature alignment.

Table 1. CIP-015-1 Requirements

CIP-015-1 Requirement Language	Dragos Platform Capabilities to Satisfy Compliance Requirements	Dragos Platform Capabilities Extending Beyond Compliance Requirements
R1.1: Monitor Network Activity Data Feeds Including Connections, Devices, and Communications	Multiple sensor deployments within an environment can support various network infrastructure collection capabilities and network activity intelligence to ingest ICS-specific communications protocols, connection monitoring, and device-specific information.	Capability for expanded sensor and collector architecture visible through common Platform analyst dashboards consuming multiple sensor feeds and collection types.
R1.2: Detection of Anomalous Network Activity	Indicator and behavior detection capabilities driven by indicators of compromise (IoCs) and TTPs, respectively. These detective capabilities are looking for known adversary activity. In addition to these historical detection approaches, the Platform also has capabilities for established baseline deviations as well as monitoring for abnormal patterns or the absence of normal patterns within a system. **Anomaly-Based Detections**[5] · Modeling detections · Configuration detections	Although "anomalous" has not been defined by NERC, it is important to have flexibility in a particular solution to accommodate changing compliance interpretations and anticipated solution implementations. In addition, stacking detection capabilities can make adversary evasion more challenging. **Intelligence-Driven Detections** • Indicators/IoC detections • Threat behavioral detections
R1.3: Evaluate Anomalous Network Activity	With multiple detection capabilities enabled in the Platform, it is essential for an analyst to have the tools to evaluate detections. The Platform contains a robust analyst threat detection dashboard. · Active IoC Dashboard · Detections Panel showing the four types of threat detections (i.e., Modeling, Threat Behavior, Configuration, and Indicator)	Although the requirement language specifies the need for an evaluation capability, it does not specify what that process looks like. This depth of analysis approach is beyond the requirement language, but here lies the uniqueness of the Platform: It connects trained personnel to the right data and approaches to enable them to act on the information. It leverages the threat detection capabilities, further integrating the expert playbooks and case management tools provided in the Platform and ultimately equipping threat hunters and incident responders with insights they can add to their operational environment knowledge. Some additional analysis capabilities and resources are also available through: • Detailed raw historical evidence collected • Industry-leading ICS/OT threat intelligence reports • OT Watch Threat Hunting as a Service • Neighborhood Keeper—collective intelligence network sending trusted insight response messages to alert regarding trends
R2: Data Retention	Collecting and storing network activity data feeds in support of Requirement 1 is a core capability of the Platform sensor, collector, and SiteStore architecture. Sizing and throughput will be determined by each entity and Dragos engineering.	Although the retention periods are not clear and, in some cases, would be inferred from the entity-specific Requirement 1 associated processes, dataset sizing and associated online/offline storage retention requirements are expandable.
R3: Data Protection	The act of ingesting network activity data feeds off the network and into a sensor, collector, and Platform solution will provide some measures to minimize the likelihood of an attacker removing evidence because there would be multiple locations to manipulate, and the act of performing the evidence removal would also generate further detections.	The Platform provides the capability to establish a case and provide retention requirements around datasets included within the case.

[5] "Key Insights for NERC CIP-015 Compliance: Anomaly Detection vs. Detecting Anomalous Activity," www.dragos.com/blog/nerc-cip-015-compliance-detect-anomalous-activity-with-dragos-platform

Four Types of Threat Detection with the Dragos Platform

Dragos uses four types of threat detection to provide a comprehensive security solution to detect and respond to potential adversarial activity (see Table 2). By integrating these four types of threat detection, the Dragos Platform enhances your ability to meet NERC CIP-015-1 requirements. This comprehensive approach not only detects anomalous activities but also provides the context to evaluate the detections and, thus, enables users to respond effectively, reduce unnecessary alerts, and enhance threat detection accuracy.

Table 2. Dragos's Four Types of Threat Detection

CIP-015-1 Requirement Language	Dragos Platform Capabilities to Satisfy Compliance Requirements	Dragos Platform Capabilities Extending Beyond Compliance Requirements
Intelligence Driven: Behavioral Detection	Codifies malicious adversary tradecraft for detection regardless of specific indicators such as malware, capability, or infrastructure. These relate to TTPs identified with specific threat groups or tool sets. These can include atomic threat behaviors (singular detections) and composite threat behaviors (multiple detections happening together).	Provides high confidence and immediate transparency for analysts to diagnose the alert against expected behavior. Enables automatic investigation and easily integrates into defensive playbooks.
Intelligence Driven: Indicators Detections	Indicators detections are specific attributes or pieces of evidence that identify malicious activities known as indicators of compromise (IoCs) based on previously observed threat data.	Indicators can be easily searched for context to quickly identify known threat activity. Can be utilized to properly prioritize and respond to activity observed.
Anomaly Based: Configuration Detections	The Dragos Platform builds a baseline of communications and devices within the environment. Configuration detections alert on deviations from a known architecture or changes to the established baseline.	Configuration detections are mostly leveraged by security personnel for threat hunting or forensic examination in conjunction with other detections.
Anomaly Based: Modeling Detections	Modeling detections detect threats by defining what is "normal" and measuring against divergence.	When detecting changes from the normal, it can detect malicious actions and abnormal behavior identifying misconfigurations or failing assets. Modeling detections are effective at identifying novel or zero-day threats that do not match known indicators.

Reviewing the CIP-015-1 Requirement mapping to Dragos Platform feature capabilities should provide entities with confidence that the solution can be implemented and operated in a manner that satisfies the compliance and cybersecurity obligations. An appropriate implementation and a successful long-term program will rely heavily on knowledgeable trained personnel. Entities should consider representatives from across their diverse workforce of engineers, operators, IT and OT professionals, cybersecurity practitioners, compliance personnel, cyber threat intel analysts, and threat hunters integral to the process. Asset owners and operators considering vendors and solution providers in this space also should look for organizations like Dragos that have invested in a diverse workforce with experienced practitioners who have worked in these same roles for other entities and now have the focus and experience to implement this capability across numerous organizations.

The Road Ahead

Looking ahead at the likely next steps of the CIP-015 journey can be a daunting (and disappointing) task if you are seeking absolute certainty. The current CIP-015-1 Standard has received FERC-proposed approval with directed changes. The FERC Notice of Proposed Rulemaking provides a significant amount of certainty in regard to requirement specifics that allows industry to begin moving down a path toward implementation. The *uncertainty* that has been introduced with the FERC Notice of Proposed Rulemaking and directed changes pertains to two areas:

- Requirement applicability
- Timing of compliance effective dates

The requirement applicability-related changes from FERC include directed changes to expand the CIP-015-1 Standard to include EACMS as well as PACS that reside outside the ESP. FERC commented that the existing CIP-015-1 Standard only applies INSM Requirements within identified ESPs. FERC stated:

> By restricting the implementation of INSM to within the electronic security perimeter, a reliability and security gap remains by not implementing INSM for the entire CIP-networked environment, i.e., outside the electronic security perimeter inclusive of EACMS and PACS. To address this gap, we propose to direct NERC to develop modifications to the proposed Reliability Standard to include EACMS and PACS, thereby protecting the reliability and security of all trust zones of the CIP-networked environment.

As a result, the CIP-015-1 Standard will undergo a revision to modify applicability language to include EACMS and PACS for High and Medium Impact assets.

The timing of compliance effective dates will be bound to the Standards development process ahead, which includes a 60-day open comment period to the Notice of Proposed Rulemaking issued on September 19, 2024, and appearing in the Federal Register on September 27, 2024. This could lead to a FERC Final Order on CIP-015-1 in the first or second quarter of 2025. The proposed CIP-015-1 implementation plan would place compliance effective dates for High and Medium Impact with ERC Control Centers in 2028 and for other Medium Impact (with ERC) facilities in 2030.

The additional consideration on timing is related to the proposed directed changes and the need to make these changes within 12 months of the final rule. Looking ahead, this would introduce a CIP-015-2 prior to the effective date of CIP-015-1. When this has occurred in the past (as it did with CIP v4 Standards and CIP v5 Standards), it has resulted in FERC directing industry to move directly to a new implementation plan that is in line with the latest approved version. This could potentially result in an extended implementation plan targeting CIP-015-2 compliance dates that are further out than if the version 1 implementation plan must be met.

Although there is some uncertainty, there is significantly more information contained within the FERC Notice of Proposed Rulemaking that is actionable now.

CIP-015 Action Items

As entities review a new set of requirements that have been introduced through Standards development, they often perform a gap analysis to determine what their current capabilities are and what actions they will need to achieve prior to the compliance date when the requirements go into effect. With the current path ahead, entities have a clear vision of what will be required and can begin considering how they will achieve the compliance requirements across capital projects and ongoing process implementation. Acknowledging the staggered implementation plan of CIP-015-1 and the ongoing Standards development activities toward CIP-015-2, entities will need to pursue a prioritized set of next steps that is informed by their unique asset mix.

Actions to take now:

- Review current list of High Impact and Medium Impact (with ERC) facilities.
- Identify existing data collection capabilities within ESPs.
- Consider the feasibility of performing network activity data feed collection from existing network infrastructure.
- Identify where the analysis task of evaluating detected anomalous activity would be performed.
- Begin evaluating potential solutions that best fit in your environment.
- Prioritize projects across High and Medium Impact Control centers with ERC.

Next steps:

- Develop a workforce plan addressing gaps in job roles and staffing levels. Where appropriate, provide necessary training to develop individuals key to project and program initiatives.
- Leverage existing test environments to evaluate solutions or configure solution detection capabilities.
- Develop processes supporting CIP-015-1 Requirements 1.1–1.3.
- Establish playbooks and case management tools in support of Requirement 1.3.
- Conduct active cybersecurity vulnerability assessments (CVAs) in a test environment as required by CIP-010. The active CVA will trigger baseline deviations, effectively testing CIP-015 anomaly detection controls.
- Consider projects across other Medium Impact facilities with ERC.
- Consider implementation needs for the requirements with expanded applicability to EACMS and PACS.

Continuously monitor and contribute:

- Participate in further industry activity on the directed changes from FERC to CIP-015-1.
- Review all systems currently identified as EACMS and PACS, and then consider implementation of CIP-015-1 requirements for those CIP-networked environments.
- Participate in Regional Entity collaboration and outreach efforts focused on CIP-015-1.
- If necessary, participate in industry collaboration activity on risk-based data feed selection approaches and consistent treatment of the term "anomalous" across entities.
- If appropriate for your entity, work with regulatory affairs staff to pursue early implementation of INSM projects, staffing, training, and identifying lessons learned under the FERC Order 893[6] incentive-based rate treatment for investment in advanced cybersecurity technologies.

Conclusion

The electric sector in North America has made consistent advances in cybersecurity capabilities and maturity over the past 20 years, but adversary capabilities and maturity have advanced as well. The Standards are not keeping pace with adversary techniques used to evade traditional security control detection. In their essential role, FERC has identified this gap in security collection, detection, and evaluation and issued directives to the industry to implement INSM capabilities within the most critical of our nation's critical infrastructure networks. Although the Standards development process can introduce regulatory lag, it also ensures the voice of industry. It has produced a set of requirements responsive to the FERC directives that can be acted upon by entities immediately with low risk and, for some entities, pursued with FERC-supported incentives.

Sponsor

SANS would like to thank this paper's sponsor:

DRAGOS

[6] "Incentives for Advanced Cybersecurity Investment," E-1-RM22-19-000, www.ferc.gov/media/e-1-rm22-19-000-0