NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Internal Network Security Monitoring

Request for Data or Information

May 25, 2023

RELIABILITY | RESILIENCE | SECURITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface iii
Introduction iv
Background iv
Due Date and NERC Contact Information v
Authority 1
Section 215 of the Federal Power Act and FERC Regulations 1
NERC Rules of Procedure 1
Applicability, Data Handling and Estimated Burden 4
How the data will be used 4
Why the data is necessary 4
How the data will be collected and validated 4
Reporting Entities 4
Due date for the information 4
Restrictions on disseminating data (Confidential/CEII) 5
Estimate on burden imposed to collect data 5
Data Request 6
Internal Network Security Monitoring Data Request 6
Example Response 10

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators participate in another.

MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Introduction

In accordance with Section 1600 of the NERC Rules of Procedure,[1] NERC may request data or information that is deemed necessary to meet its obligations under Section 215 of the Federal Power Act[2], as authorized by Section 39.2(d) of the Federal Energy Regulatory Commission's (FERC) regulations. This is such a request.

This request was developed in accordance with the expedited procedures provided in Section 1606 of the NERC Rules of Procedure. Section 1606 allows for a shortened time period for posting a draft request for data or information for comment if the data or information must be obtained in order to evaluate a threat to the reliability or security of the BPS or in order to comply with a directive in an order issued by FERC or another governmental authority.

Background

On January 19, 2023, FERC directed NERC in Order No. 887 to develop and submit for Commission approval by July 9, 2024 new or modified Reliability Standards that require Internal Network Security Monitoring[3] (INSM) within a trusted Critical Infrastructure Protection (CIP) networked environment for all high impact Bulk Electric System (BES) Cyber Systems with and without external routable connectivity (ERC) and medium impact BES Cyber Systems with ERC.

Further, Order No. 887 directs NERC to perform a study to support possible future Commission actions on whether to extend INSM requirements to medium impact BES Cyber Systems without ERC and all low impact BES Cyber Systems regardless of ERC status[4]. Data collected to perform the study will be used to inform an analysis regarding the substantive risks posed by these BES Cyber Systems operating without the implementation of INSM. The study is required to include a determination of:

(1) Ongoing risk to the reliability and security of the Bulk-Power System (BPS) posed by low and medium impact BES Cyber Systems that would not be subject to the new or modified Reliability Standards, including the number of low and medium impact BES Cyber Systems not required to comply with the new or modified standard; and

(2) Potential technological or other challenges involved in extending INSM to additional BES Cyber Systems, as well as possible alternative mitigating actions to address ongoing risks.

In support of the study NERC is collecting data from registered entities regarding the following:

- Quantity of substation and generation locations that contain medium impact BES Cyber Systems with ERC.
- Quantity of substation and generation locations that contain medium impact BES Cyber Systems without ERC.
- Quantity of low impact locations (including a breakdown by substations, generation resources, and Control Centers that contain low impact BES Cyber Systems without ERC.
- Quantity of low impact locations (including a breakdown by substations, generation resources, and Control Centers) that contain low impact BES Cyber Systems with ERC.

[1] NERC's Rules of Procedure are available at: Rules Of Procedure - All Documents (nerc.com)
[2] 16 U.S.C § 824o" (Section 215)
[3] 1 Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems, Order No. 887, 182 FERC ¶ 61,021 (Jan. 19, 2023) [hereinafter Order No. 887], https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20230119-3085&optimized=false. Per Order No. 887 at P 9, INSM consists of three stages: (1) collection; (2) detection; and (3) analysis.
[4] As it pertains to low impact BES Cyber System, ERC is being used in the context of this data request to refer to external connectivity to/from the BES Cyber System although the defined term is not used in association with low impact BES Cyber System within the NERC CIP standards.

- Identify the potential technological, logistical, or other challenges involved in extending INSM to additional BES Cyber Systems.
- Identify possible alternative actions to mitigate the risk posed by these BES Cyber Systems operating without the implementation of INSM.

For the purposes of this data request, the term "location" refers to physical space associated with an asset. A location may include any number of BES Cyber Systems at a given asset.

The Commission directed NERC to submit the study by January 18, 2024 (within 12 months of the issuance of Order No. 887).

Due Date and NERC Contact Information

The completion of this data request and submission to NERC is due within 60 days after issuance of the data request.

Authority

This section describes the statute, regulations, and governing procedures that grant NERC its authority to issue this data request.

Section 215 of the Federal Power Act and FERC Regulations

Under Section 215 of the Federal Power Act (16 U.S.C. § 824o), Congress entrusted FERC with the duties of approving and enforcing rules to ensure the reliability of the nation's BPS, and with the duties of certifying an Electric Reliability Organization that would be charged with developing and enforcing mandatory Reliability Standards, subject to FERC approval. NERC was certified as the ERO on July 20, 2006. In addition to NERC's authority derived from Section 215 of the Federal Power Act, NERC is requesting this information in accordance with its authority provided in 18 C.F.R. §39.2(d), which provides:

> *Each user, owner or operator of the Bulk-Power System within the United States (other than Alaska and Hawaii) shall provide the Commission, the Electric Reliability Organization and the applicable Regional Entity such information as is necessary to implement section 215 of the Federal Power Act as determined by the Commission and set out in the Rules of the Electric Reliability Organization and each applicable Regional Entity. The Electric Reliability Organization and each Regional Entity shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act.*

NERC Rules of Procedure

Section 1600 of the NERC Rules of Procedure provides a mechanism for requesting data or information from registered entities, which includes an expedited procedure. On February 16, 2023, the NERC Board of Trustees authorized a request to use the expedited procedures for this data request.[5] The NERC Rules of Procedure Section 1600 provides in pertinent part:

> ***1601. Scope of a NERC or Regional Entity Request for Data or Information***
> *Within the United States, NERC and Regional Entities may request data or information that is necessary to meet their obligations under Section 215 of the Federal Power Act, as authorized by Section 39.2(d) of the Commission's regulations, 18 C.F.R. § 39.2(d). In other jurisdictions NERC and Regional Entities may request comparable data or information, using such authority as may exist pursuant to these Rules of Procedure and as may be granted by Applicable Governmental Authorities in those other jurisdictions. The provisions of Section 1600 shall not apply to Requirements contained in any Reliability Standard to provide data or information; the Requirements in the Reliability Standards govern. The provisions of Section 1600 shall also not apply to data or information requested in connection with a compliance or enforcement action under Section 215 of the Federal Power Act, Section 400 of these Rules of Procedure, or any procedures adopted pursuant to those authorities, in which case the Rules of Procedure applicable to the production of data or information for compliance and enforcement actions shall apply.*
>
> ***1602. Procedure for Authorizing a NERC Request for Data or Information***
>
> *****
>
> *2.1. A proposed request for data or information shall contain, at a minimum, the following information: (i) a description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC*

[5] NERC Board of Trustees Meeting, Agenda Item 9d (Feb. 16, 2023), at Board_Open_Meeting_Agenda_Package_February_16_2023.pdf (nerc.com)
https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting_Agenda_Package_February_16_2023.pdf.

to meet its obligations under applicable laws and agreements; (ii) a description of how the data or information will be collected and validated; (iii) a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("Reporting Entities"); (iv) the schedule or due date for the data or information; (v) a description of any restrictions on disseminating the data or information (e.g., "Confidential Information," "Critical Energy Infrastructure Information," "aggregating" or "identity masking"); and (vi) an estimate of the relative burden imposed on the Reporting Entities to accommodate the data or information request.

2.2. A proposed modification to a previously authorized request for data or information shall explain (i) the nature of the modifications; (ii) an estimate of the burden imposed on the Reporting Entities to accommodate the modified data or information request, and (iii) any other items from Section 1602.2.1 that require updating as a result of the modifications.

3. *After the close of the comment period, NERC shall make such revisions to the proposed request for data or information as are appropriate in light of the comments. NERC shall submit the proposed request for data or information, as revised, along with the comments received, NERC's evaluation of the comments and recommendations, to the Board of Trustees.*
4. *In acting on the proposed request for data or information, the Board of Trustees may authorize NERC to issue it, modify it, or remand it for further consideration.*
5. *NERC may make minor changes to an authorized request for data or information without Board approval. However, if a Reporting Entity objects to NERC in writing to such changes within 21 days of issuance of the modified request, such changes shall require Board approval before they are implemented.*
6. *Authorization of a request for data or information shall be final unless, within thirty (30) days of the decision by the Board of Trustees, an affected party appeals the authorization under this Section 1600 to the Applicable Governmental Authority.*

1606. Expedited Procedures for Requesting Time-Sensitive Data or Information

1. *In the event NERC or a Regional Entity must obtain data or information by a date or within a time period that does not permit adherence to the time periods specified in Section 1602, the procedures specified in Section 1606 may be used to obtain the data or information. Without limiting the circumstances in which the procedures in Section 1606 may be used, such circumstances include situations in which it is necessary to obtain the data or information (in order to evaluate a threat to the reliability or security of the Bulk Power System, or to comply with a directive in an order issued by the Commission or by another Applicable Governmental Authority) within a shorter time period than possible under Section 1602. The procedures specified in Section 1606 may only be used if authorized by the NERC Board of Trustees prior to activation of such procedures.*
2. *Prior to posting a proposed request for data or information, or a modification to a previously-authorized request, for public comment under Section 1606, NERC shall provide the proposed request or modification, including the information specified in paragraph 1602.2.1 or 1602.2.2 as applicable, to the Commission's Office of Electric Reliability. The submission to the Commission's Office of Electric Reliability shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information. The submission shall be made to the Commission's Office of Electric Reliability as far in advance, up to twenty-one (21) days, of the posting of the proposed request or modification for public comments as is reasonably possible under the circumstances, but in no event less than two (2) days in advance of the public posting of the proposed request or modification.*

3. *NERC shall post the proposed request for data or information or proposed modification to a previously-authorized request for data or information for a public comment period that is reasonable in duration given the circumstances, but in no event shorter than five (5) days. The proposed request for data or information or proposed modification to a previously-authorized request for data or information shall include the information specified in Section 1602.2.1 or 1602.2.2, as applicable, and shall also include an explanation of why it is necessary to use the expedited procedures of Section 1606 to obtain the data or information.*

4. *The provisions of Sections 1602.3, 1602.4, 1602.5 and 1602.6 shall be applicable to a request for data or information or modification to a previously-authorized request for data or information developed and issued pursuant to Section 1606, except that (a) if NERC makes minor changes to an authorized request for data or information without Board approval, such changes shall require Board approval if a Reporting Entity objects to NERC in writing to such changes within five (5) days of issuance of the modified request; and (b) authorization of the request for data or information shall be final unless an affected party appeals the authorization of the request by the Board of Trustees to the Applicable Governmental Authority within five (5) days following the decision of the Board of Trustees authorizing the request, which decision shall be promptly posted on NERC's website.*

Applicability, Data Handling and Estimated Burden

This section describes the entity applicability, data necessity, data handling procedures and estimated burden associated with this data request.

How the data will be used

The data will be used by NERC staff to develop a study determining: (1) Ongoing risk to the reliability and security of the BPS posed by low and medium impact BES Cyber Systems that would not be subject to the new or modified Reliability Standards; and (2) Potential technological or other challenges involved in extending INSM to additional BES Cyber Systems, as well as possible alternative mitigating actions to address ongoing risks.

Why the data is necessary

The collected data and information is necessary for NERC to meet its obligations under applicable laws and agreements, specifically the FERC directive to conduct a study assessing the substantive risks posed by certain BES Cyber Systems operating without the implementation of INSM.

How the data will be collected and validated

Primary Compliance Contacts (PCC) for reporting entities must respond by logging onto the ERO portal and selecting "INSM Data Request" at the top of the page. If you do not see an "INSM Data Request" option at the top of the page, you are not a PCC for a reporting entity. For those reporting entities that have more than one PCC, all PCCs will have access to the response. Reponses can be saved and modified repeatedly but once submitted the responses are final. Portal responses are protected and available to ERO study participants on a need to know basis only. NCER will compare the list of registered entities with the data request respondents to ensure that responses are received as requested.

Any questions may be directed to: INSM_DR_Info@nerc.com.

Reporting Entities

- Balancing Authorities
- Distribution Providers
- Generator Owners
- Generator Operators
- Reliability Coordinators
- Transmission Owners
- Transmission Operators
- Distribution Providers[6]

Due date for the information

Reporting entities are expected to respond to the data request within sixty days of its issuance.

[6] Limited to Distribution Providers that have certain facilities listed in the applicability section of the CIP standards

Restrictions on disseminating data (Confidential/CEII)

NERC does not anticipate requesting specific information relative to BES Cyber Systems that would create the need to invoke Critical Electric Infrastructure Information confidentiality provisions of the NERC Rules of Procedure. Additionally, NERC will not make public entity specific information collected through this data request. Should responding entities determine their response invokes Critical Electric Infrastructure Information confidentiality provisions, NERC will address the data collected on a case-by-case basis to ensure appropriate data handling.

Estimate on burden imposed to collect data

This is a one-time data request providing a count of medium Impact locations without ERC and low impact locations with and without ERC. Additionally, registered entities are required to provide an estimate of the network configurations by type at low impact locations. All counts are given by location and network configuration data should be known to entities; neither of which require complex mining of information or analytics to resolve. The remaining questions are optional and rely on the professional judgement, expertise, and experience of registered entity staff. The estimated time to complete the data request will vary with the size of the entity, but is estimated to average less than 150 hours total per entity.

Data Request

DATA REQUEST QUESTIONS ARE PROVIDED HERE FOR INFORMATION PURPOSES ONLY. All RESPONSES MUST BE PROVIDED THROUGH THE ERO PORTAL.

Internal Network Security Monitoring Data Request

For questions requiring estimates (7, 8, and 10), entities should provide their best estimates using the data they have available.

Please answer the following questions.

Responsible Entity Questions:

1. What is the NERC Compliance Registry (NCR) number and Region(s) for which you are reporting under this Data Request?
    a. NCR:
    b. Region(s):
2. Entity contact information
    a. Name:
    b. Title:
    c. Email address:
    d. Contact number:
3. (Required Response) Provide the number of (a) substation and (b) generation locations containing medium impact BES Cyber Systems **with** ERC[7]. (Comment field can be used to provide explanation for responses if needed.)
    a. << numerical value >>
    b. << numerical value >>
    c. << Comment >> Optional
4. (Required Response) Provide the number of (a) substation and (b) generation locations containing medium impact BES Cyber Systems **without** ERC. (Comment field can be used to provide explanation for responses if needed.)
    a. << numerical value >>
    b. << numerical value >>
    c. << Comment >> Optional
5. (Required Response) Provide the number of (a) substation, (b) generation, and (c) Control Center locations containing low impact BES Cyber Systems **with** ERC. (Comment field can be used to provide explanation for responses if needed.)
    a. << numerical value >>
    b. << numerical value >>

[7] As it pertains to low impact BES Cyber System, ERC is being used in the context of this data request to refer to external connectivity to/from the BES Cyber System although the defined term is not used in association with low impact BES Cyber System within the NERC CIP standards.

c. << numerical value >>

d. << Comment >> Optional

6. (Required Response) Provide the number of (a) substation, (b) generation, and (c) Control Center locations containing low impact BES Cyber Systems **without** ERC. (Comment field can be used to provide explanation for responses if needed.)

   a. << numerical value >>

   b. << numerical value >>

   c. << numerical value >>

   d. << Comment >> Optional

7. (Required Response) Provide the estimated percentages, totaling 100%, of network configurations for your medium impact BES Cyber Systems **without** ERC.

   a. Completely IP-based

      << numerical value >>

   b. Majority IP-based with minimal serial (or other non-IP connectivity)

      << numerical value >>

   c. Completely serial (or other non-IP connectivity)

      << numerical value >>

   d. Majority serial (or other non-IP connectivity) with minimal IP-based connectivity

      << numerical value >>

   e. Approximately 50/50 mix of IP-based and serial (or other non-IP connectivity) present at location

      << numerical value >>

8. (Required Response) Provide the estimated percentages, totaling 100%, of network configurations for your low impact BES Cyber Systems.

   a. Completely IP-based

      << numerical value >>

   b. Majority IP-based with minimal serial (or other non-IP connectivity)

      << numerical value >>

   c. Completely serial (or other non-IP connectivity)

      << numerical value >>

   d. Majority serial (or other non-IP connectivity) with minimal IP-based connectivity

      << numerical value >>

   e. Approximately 50/50 mix of IP-based and serial (or other non-IP connectivity) present at location

      << numerical value >>

9. (Required Response) From (1) least challenging to (5) most challenging, independently rate each of the listed potential technological, logistical, or other challenges involved in extending INSM to additional medium impact BES Cyber Systems (e.g., medium impact without ERC) and low impact BES Cyber Systems (e.g., all low impact):

a. (Required Response) Implementation of INSM may require equipment retrofit and network redesign.

<< For medium impact without ERC - Rate (1-5): numerical value >>

<< For low impact - Rate (1-5): numerical value >>

<< Comment >> Optional

b. (Required Response) Compliance burden associated with implementing INSM (e.g., lack of a discrete list of low impact BES Cyber Systems and defined low impact electronic security perimeters).

<< For medium impact without ERC - Rate (1-5): numerical value >>

<< For low impact - Rate (1-5): numerical value >>

<< Comment >> Optional

c. (Required Response) The overall costs associated with INSM (e.g., implementation, maintenance, support).

<< For medium impact without ERC - Rate (1-5): numerical value >>

<< For low impact - Rate (1-5): numerical value >>

<< Comment >> Optional

d. (Required Response) Technical supply chain constraints (e.g., hardware/software availability).

<< For medium impact without ERC - Rate (1-5): numerical value >>

<< For low impact - Rate (1-5): numerical value >>

<< Comment >> Optional

e. (Required Response) Shortages of qualified staff (e.g., implementation, maintenance, support).

<< For medium impact without ERC - Rate (1-5): numerical value >>

<< For low impact - Rate (1-5): numerical value >>

<< Comment >> Optional

f. (Required Response) INSM implementation may require expanding ERC at some BES Cyber System locations, thereby increasing the attack surface.

<< For medium impact without ERC - Rate (1-5): numerical value >>

<< For low impact - Rate (1-5): numerical value >>

<< Comment >> Optional

g. (Optional Response) Other challenges.

Please keep answers as concise as possible.

<< For medium impact without ERC - Free form field >>

<< For low impact - Free form field >>

10. (Required Response) Provide the estimated percentage of low impact BES Cyber Systems that currently have network based malicious code detection. Malicious code detection can be accomplished either internally to the BES Cyber System network or at the BES Cyber System network boundary.

<< numerical value >>

<< Comment >> Optional

11. (Optional Response) List recommended alternative solutions or controls to mitigate the risk posed[8] to BES Cyber Systems operating without INSM. **Please keep answers as concise as possible**.
    a. << free form field >>
    b. << free form field >>
    c. << free form field >>
    d. << free form field >>
12. (Optional Response) For existing implementations of INSM at current BES Cyber System locations, what solutions (e.g., vendors, products, and service providers) are deployed? **Please provide a concise high level list**.
    a. << For high impact BES Cyber Systems - free form field >>
    b. << For medium impact BES Cyber Systems with ERC - free form field >>
    c. << For medium impact BES Cyber Systems without ERC - free form field >>
    d. << For low impact BES Cyber Systems - free form field >>

[8] See FERC Docket No. RM22-3-000; Order No. 887 Section 15

Example Response

Responsible Entity General Questions:

Responsible Entity Questions:

1. What is the NERC Compliance Registry (NCR) number and Region(s) for which you are reporting under this Data Request?
    a. NCR: NCR01111
    b. Region(s): Region1
2. Entity contact information
    a. Name: John Doe
    b. Title: Entity PCC
    c. Email address: John.Doe@ NCR01111.com
    d. Contact number: 999.555.1212
3. (Required Response) Provide the number of (a) substation and (b) generation locations containing medium impact BES Cyber Systems **with** ERC[9]. (Comment field can be used to provide explanation for responses if needed.)
    a. 30
    b. 20
    c. None
4. (Required Response) Provide the number of (a) substation and (b) generation locations containing medium impact BES Cyber Systems **without** ERC. (Comment field can be used to provide explanation for responses if needed.)
    a. 30
    b. 20
    c. None
5. (Required Response) Provide the number of (a) substation, (b) generation, and (c) Control Center locations containing low impact BES Cyber Systems **with** ERC. (Comment field can be used to provide explanation for responses if needed.)
    a. 30
    b. 20
    c. 2
    d. None
6. (Required Response) Provide the number of (a) substation, (b) generation, and (c) Control Center locations containing low impact BES Cyber Systems **without** ERC. (Comment field can be used to provide explanation for responses if needed.)
    a. 50

[9] As it pertains to low impact BES Cyber System, ERC is being used in the context of this data request to refer to external connectivity to/from the BES Cyber System although the defined term is not used in association with low impact BES Cyber System within the NERC CIP standards.

b. 30

c. 2

d. None

7. (Required Response) Provide the estimated percentages, totaling 100%, of network configurations for your medium impact BES Cyber Systems **without** ERC.

   a. Completely IP-based

      30%

   b. Majority IP-based with minimal serial (or other non-IP connectivity)

      25%

   c. Completely serial (or other non-IP connectivity)

      25%

   d. Majority serial (or other non-IP connectivity) with minimal IP-based connectivity

      15%

   e. Approximately 50/50 mix of IP-based and serial (or other non-IP connectivity) present at location

      5%

8. (Required Response) Provide the estimated percentages, totaling 100%, of network configurations for your low impact BES Cyber Systems.

   a. Completely IP-based

      30%

   b. Majority IP-based with minimal serial (or other non-IP connectivity)

      25%

   c. Completely serial (or other non-IP connectivity)

      25%

   d. Majority serial (or other non-IP connectivity) with minimal IP-based connectivity

      15%

   e. Approximately 50/50 mix of IP-based and serial (or other non-IP connectivity) present at location

      5%

9. (Required Response) From (1) least challenging to (5) most challenging, independently rate each of the listed potential technological, logistical, or other challenges involved in extending INSM to additional medium impact BES Cyber Systems (e.g., medium impact without ERC) and low impact BES Cyber Systems (e.g., all low impact):

   a. (Required Response) Implementation of INSM may require equipment retrofit and network redesign.

      For medium impact without ERC - Rate (1-5): 5

      For low impact - Rate (1-5): 3

      Comment: None

   b. (Required Response) Compliance burden associated with implementing INSM (e.g., lack of a discrete list of low impact BES Cyber Systems and defined low impact electronic security perimeters).

For medium impact without ERC - Rate (1-5): 5

For low impact - Rate (1-5): 2

Comment: None

c. (Required Response) The overall costs associated with INSM (e.g., implementation, maintenance, support).

For medium impact without ERC - Rate (1-5): 5

For low impact - Rate (1-5): 4

Comment: None

d. (Required Response) Technical supply chain constraints (e.g., hardware/software availability).

For medium impact without ERC - Rate (1-5): 5

For low impact - Rate (1-5): 3

Comment: None

e. (Required Response) Shortages of qualified staff (e.g., implementation, maintenance, support).

For medium impact without ERC - Rate (1-5): 5

For low impact - Rate (1-5): 3

Comment: None

f. (Required Response) INSM implementation may require expanding ERC at some BES Cyber System locations, thereby increasing the attack surface.

For medium impact without ERC - Rate (1-5): 5

For low impact - Rate (1-5): 3

Comment: None

g. (Optional Response) Other challenges.

Please keep answers as concise as possible.

For medium impact without ERC – My entity anticipates XYZ challenge.

For low impact - My entity anticipates XYZ challenge.

10. (Required Response) Provide the estimated percentage of low impact BES Cyber Systems that currently have network based malicious code detection. Malicious code detection can be accomplished either internally to the BES Cyber System network or at the BES Cyber System network boundary.

    a. 30

    b. No comment

11. (Optional Response) List recommended alternative solutions or controls to mitigate the risk posed[10] to BES Cyber Systems operating without INSM. **Please keep answers as concise as possible**.

    a. My entity recommends alternative XYZ to mitigate risk.

    b. My entity recommends alternative FGH to mitigate risk.

    c. None

[10] See FERC Docket No. RM22-3-000; Order No. 887 Section 15

d. None

12. (Optional Response) For existing implementations of INSM at current BES Cyber System locations, what solutions (e.g., vendors, products, and service providers) are deployed? **Please provide a concise high level list**.

    a. For high impact BES Cyber Systems – Solution XYZ from vendor ZYX.

    b. For medium impact BES Cyber Systems with ERC – My Entity developed internal solution ZDF.

    c. For medium impact BES Cyber Systems without ERC – My entity is using a partial solution leveraging XYZ….

    d. For low impact BES Cyber Systems – No solution implemented by my entity.