UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Version 5 Critical Infrastructure Protection Reliability Standards	**)** **)**	**Docket No. RM13-5-___**

INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION REGARDING THE BES CYBER ASSET SURVEY

Pursuant to Order No. 791,[1] the North American Electric Reliability Corporation ("NERC") hereby submits to the Federal Energy Regulatory Commission ("FERC" or "Commission"), for informational purposes, an assessment of the results of the survey regarding the scope of assets subject to the definition of the term "BES Cyber Asset," as that definition was approved by the Commission in Order No. 791 and included in the Glossary of Terms Used in NERC Reliability Standards ("NERC Glossary").

I. INTRODUCTION

On November 22, 2013, FERC issued Order No. 791, approving new and modified Critical Infrastructure Protection ("CIP") Reliability Standards, collectively referred to as the CIP version 5 standards, as well as new and modified definitions for NERC Glossary terms used in the CIP version 5 standards. Among others, FERC approved definitions for the terms "BES Cyber System" and "BES Cyber Asset." The CIP version 5 standards are designed to mitigate the cybersecurity risks to the reliable operation of the Bulk-Power System by requiring entities to take measures to protect their BES Cyber Systems, which, by definition, consist of one or more BES

[1] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 at PP 122-125 (2013), *Order on Clarification and Rehearing*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

Cyber Assets.[2] As discussed below, BES Cyber Assets are those Cyber Assets (i.e., programmable electronic devices) that, if compromised, could have adverse effects on the real-time operation of the Bulk Electric System ("BES") (i.e., within 15 minutes of the Cyber Asset's required operation, misoperation, or non-operation).

The identification of BES Cyber Assets is thus a foundational step to applying the protections of the CIP Reliability Standards. It is therefore important, as the Commission recognized, to understand the scope of the term "BES Cyber Asset" to ensure that entities are properly and consistently determining the types of Cyber Assets that would fall within the BES Cyber Asset definition.[3] To that end, although the Commission approved the definition of "BES Cyber Asset," it directed NERC to conduct a survey of Cyber Assets that are included or excluded under the definition, particularly as a result of the application of the 15-minute parameter.[4] The Commission also directed NERC to submit an informational filing explaining, based on the results of the survey, the following items: (1) specific ways in which entities determine which Cyber Assets meet the 15-minute parameter; (2) types or functions of Cyber Assets that do not fall within the BES Cyber Asset definition and the rationale for such determinations; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from Regional Entities on lessons learned with the application of the BES Cyber Asset definition.

As discussed below, to complete the survey, NERC requested that the participants in NERC's Implementation Study for the CIP Version 5 Transition Program (the "Implementation

---

[2] As defined in the NERC Glossary, a BES Cyber System is "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."

[3] *See* Order No. 791 at PP 123-124.

[4] As explained below, a BES Cyber Asset is "a Cyber Asset that if rendered unavailable, degraded, or misused would, *within 15 minutes of its required operation, misoperation, or non-operation*, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System." (Emphasis added).

Study") provide a description of: (1) their process for determining whether a Cyber Asset meets the definition of BES Cyber Asset; (2) challenges they faced or common problem areas they identified in making such determinations; and (3) the types or functions of Cyber Assets that are included or excluded from being designated as BES Cyber Assets and the rationale for the inclusion or exclusion. The Implementation Study participants were best suited to form the basis for the survey because they had begun the process of identifying their BES Cyber Assets and implementing certain elements of the CIP version 5 standards with the guidance of NERC and the Regional Entities. Using the Implementation Study participants thus helped ensure that the responses to the survey were meaningful and reflected an operational application of the BES Cyber Asset definition.

The survey provided NERC an opportunity to assess the application of the BES Cyber Asset definition and identify any areas of concern. As explained in greater detail below, the results of the survey indicate that, in general, the application of the BES Cyber Asset definition, and the 15-minute parameter in particular, resulted in the identification of BES Cyber Assets consistent with the language and intent of the CIP version 5 standards as well as NERC's expectations. The survey demonstrates that the definition of BES Cyber Asset provides a sound basis for identifying the types of Cyber Assets that need the cybersecurity protections required by the CIP Reliability Standards.

As expected, the results of the survey show that a determination of whether a particular Cyber Asset is a BES Cyber Asset is necessarily dependent on facts and circumstances, namely, the function performed by the Cyber Asset and whether that function is integral to real-time operations. Nevertheless, as discussed below, there was significant commonality in the types and functions of Cyber Assets that the Implementation Study participants designated as BES Cyber

Assets and the rationale for excluding particular Cyber Assets. As to the 15-minute parameter, the Implementation Study participants reported that the application of that parameter was straightforward, stating that if a Cyber Asset could have an adverse impact on real-time reliability, it would have a near immediate impact, leaving little ambiguity as to whether it meets the 15-minute parameter.

While the results of the survey did not indicate a need to modify the BES Cyber Asset definition, the survey did highlight specific areas where NERC should provide industry additional guidance to help ensure that responsible entities are properly and consistently applying the BES Cyber Asset definition. As described below, the Implementation Study participants identified certain challenges they faced in trying to apply the definition in an efficient and consistent manner. Based on the results of the survey, NERC also identified certain discrepancies in the application of the BES Cyber Asset definition. Ultimately, NERC, the Regional Entities, and the Implementation Study participants concluded that the discrepancies and challenges were not necessarily the result of a flaw in the BES Cyber Asset definition but in the practical application of the definition, which the Electric Reliability Organization ("ERO")[5] could address through providing additional guidance to industry stakeholders. NERC is currently working with the Implementation Study participants and the Regional Entities to develop lessons learned from the survey to share with the broader stakeholder community through various mechanisms, including guidance documents, training workshops, and other targeted outreach efforts.

Section II of this informational filing provides additional background on the development of the BES Cyber Asset definition. Section III discusses the manner in which NERC

[5] NERC was certified by the Commission as the ERO, pursuant to §215(c) of the Federal Power Act and Commission order issued July 20, 2006; *Order Certifying the North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006).

conducted the survey. Finally, Section IV discusses the results of the survey, providing information on each of the four items the Commission directed NERC to explain in the informational filing.

II. BACKGROUND

In Order No. 791, FERC approved the following definition for the term "BES Cyber Asset."[6]

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an [Electronic Security Perimeter ("ESP")], a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

As the Commission discussed in Order No. 791, the definition "is intended to capture assets involved in real-time operations, such as systems that provide input to an operator for real-time operations or trigger automated real-time operations."[7] Because of the potential impact on real-time operations if such Cyber Assets were compromised, it is these types of Cyber Assets that require the cybersecurity protections required by the CIP Reliability Standards. The definition of BES Cyber Asset, and the 15-minute parameter in particular, is not about detecting and responding to a cybersecurity incident within 15 minutes; instead, it is designed to identify those Cyber Assets that, when needed in real-time, could adversely impact the reliable operation of the BES if those Cyber Assets were unavailable, misused, or degraded as a result of a cyber-attack.[8]

---

6 Order No. 791 at P 122.

7 Order No. 791 at P 122.

8 The 15-minute parameter is essentially a measurable proxy for real-time operations in the CIP context.

In the Commission's Notice of Proposed Rulemaking ("NOPR") in this proceeding, the Commission sought comment on the purpose and effect of the proposed 15-minute parameter, including the types of assets that would fall within the definition of BES Cyber Asset, so as to better understand whether the definition would exclude Cyber Assets that are integral to reliable real-time operations.[9] In its comments to the NOPR, NERC stated:

> Examples of the assets/systems that would typically be included in the 15-minute parameter are [supervisory control and data acquisition ("SCADA") systems], Energy Management Systems [("EMS')], transmission protection systems, and generation control systems, while typical systems that might be excluded by the 15-minute parameter are systems that collect data for engineering analysis and support, and maintenance rather than providing input to the operator for real-time operations or triggering automated real-time operations. Such excluded systems would include those used to collect data for the purpose of determining maintenance schedules for assets such as transformers or for engineering analysis.[10]

NERC also explained, however, that because there are differences in the way certain Cyber Assets are used across the BES, a determination of whether a particular Cyber Asset meets the definition of a BES Cyber Asset necessarily depends upon the individual facts and circumstances of how an entity uses the Cyber Asset (i.e., the function(s) of the Cyber Asset and the Facilities, systems or equipment it supports).[11] For instance, while there are certain core systems – such as EMS/SCADA, automatic generation control ("AGC"), distributed control systems ("DCS"), relays, and remote terminal units ("RTUs") – that ordinarily support real-time reliability functions and are generally understood to be BES Cyber Systems, entities must still evaluate the functionality of those systems to determine whether the Cyber Assets that comprise those systems

---

[9] *Version 5 Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 143 FERC ¶ 61,055 (2013).

[10] *Comments of the North American Electric Reliability Corporation on the Notice of Proposed Rulemaking for Version 5 Critical Infrastructure Protection Reliability Standards* at 26-27, Docket No. RM13-5-000 (Jun. 24, 2013) ("NERC NOPR Comments").

[11] NERC NOPR Comments at 27.

would be considered BES Cyber Assets. Further, an entity can have multiples of the same type of Cyber Assets at a given location or spanning multiple locations, some of which are components of a reliability-based system while the others simply support a general corporate function. Responsible entities, NERC clarified, must therefore evaluate the function(s) performed by their various Cyber Assets to determine whether a particular Cyber Asset is used to perform or support the performance of a real-time reliability function and should be identified as a BES Cyber Asset.[12]

While the Commission approved the definition in Order No. 791, the Commission sought, given the criticality of the identification of BES Cyber Assets to the protections required by the CIP version 5 standards, to obtain more specific information about the types and functions of assets that will be included or excluded under the BES Cyber Assets definition as a result of the application of the 15-minute parameter.[13] To that end, the Commission instructed NERC to:

1. conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation period; and
2. based on the data obtained from the survey, submit an informational filing, within one year of the effective date of Order No. 791, which is February 3, 2015, explaining:
    a. specific ways in which entities determine which Cyber Assets meet the 15-minute parameter;
    b. the types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why;
    c. common problem areas or challenges entities faced when designating BES Cyber Assets; and

[12] *Id*. As an example, NERC noted that in some cases a phasor measurement unit would not be considered a BES Cyber Asset if its use is limited to providing historical data for engineering analysis. In such a scenario, it would not have a real-time reliability impact. Other entities, however, may use a phasor measurement unit to provide data for real-time operations. In that case, the phasor measurement unit would be considered a BES Cyber Asset because the asset has a real-time reliability impact.

[13] Order No. 791 at P 123.

d. feedback from each Regional Entity participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition.[14]

In Order No. 791-A, the Commission clarified:

> …Order No. 791 did not direct NERC to conduct an inventory-type survey of all Cyber Assets impacted by the 15-minute parameter. Instead, the scope of the survey was left for NERC to determine. Order No. 791 intended that NERC develop a survey of sufficient scope in order to respond to the questions posed in Order No. 791 in the required NERC informational filing. For example, NERC could use the participants in the pilot program, discussed above, as the basis for the survey.[15]

III. SURVEY PARTICPANTS AND CONTENT

a. Survey Participants

Consistent with Order Nos. 791 and 791-A, NERC worked with the participants in its Implementation Study to complete the survey. As described further in its Implementation Study Final Report,[16] NERC initiated a program, working collaboratively with the Regional Entities and industry participants, to support an industry-wide transition to the CIP version 5 standards in a manner that is timely, effective, and efficient. As part of that program, NERC conducted an Implementation Study in which industry volunteers implemented elements of the CIP version 5 standards in an accelerated time frame to help NERC and the Regional Entities understand the challenges responsible entities may face transitioning to the CIP version 5 standards. NERC conducted the Implementation Study between October 2013 and June 2014 and the final report discussing the results of the study was released in October 2014.

NERC selected the participants for the Implementation Study based on their history of successful compliance with the currently-effective CIP Reliability Standards, demonstrated

---

[14] *Id*. at P 124-25.

[15] Order No. 791-A at P 21.

[16] Available at http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf.

effective internal controls, and a willingness to commit the required resources to support the transition at an early stage. Additionally, NERC sought to ensure that the Implementation Study participants were representative of different types of responsible entities (e.g., size and location). During the Implementation Study, the participants focused on technical solutions and processes needed to implement certain aspects of the CIP version 5 standards, and they developed a deeper understanding of compliance and enforcement matters unique to the CIP version 5 standards.

The lessons learned from the Implementation Study are being shared with the broader stakeholder community through various mechanisms, including guidance documents, training workshops, and other targeted outreach efforts, designed to, among other things, accomplish the following objectives:

1. *Implementation Readiness* – Improve industry's understanding of the technical security requirements of the CIP version 5 standards to help ensure that responsible entities are technically ready to implement the CIP version 5 standards upon their effective date.
2. *Clarify Compliance and Enforcement Expectations* – Clarify expectations for compliance and enforcement of the CIP Reliability Standards, including application of NERC's risk-based compliance and enforcement program to the CIP version 5 standards.
3. *Resource Requirements* – provide industry and the Regional Entities an understanding of the technical and compliance-related resources and efforts needed to transition to and comply with the CIP version 5 standards.
4. *Consistent and Reasonable Enforcement* – Ensure that the ERO enforces the CIP version 5 standards consistently, reasonably, and transparently.[17]

For purposes of the survey, NERC determined that working with the Implementation Study participants would provide the most meaningful responses to the survey given their operational experience implementing the CIP version 5 standards during the Implementation Study. Specifically, because the Implementation Study participants had already begun the process of identifying and categorizing certain of their BES Cyber Systems according to Reliability CIP-002-

[17] Additional information on NERC's CIP version 5 transition program is available at http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx.

5.1,[18] there was greater assurance that the responses to the survey would be representative of the types and functions of Cyber Assets that responsible entities will ultimately identify as BES Cyber Assets.[19] Using the Implementation Study participants also allowed NERC to work closely with the participants to ask specific follow-up questions and understand particular details that NERC would have otherwise been unable to collect if a larger pool of registered entities participated in the survey. Because NERC selected the Implementation Study participants as a representative sample of registered entities, NERC was comfortable that the survey responses would be representative of entities of different sizes and from various regions.

In addition to surveying the Implementation Study participants, NERC requested that the Regional Entities that participated in the Implementation Study provide their feedback on any lessons learned from the Implementation Study related to the scope and application of the BES Cyber Asset definition.

b. Survey Content

Exhibit 1 hereto is a copy of the survey provided to the Implementation Study participants. The survey was designed to help NERC better understand how the Implementation Study participants identified BES Cyber Assets and to obtain the data the Commission requested in Order No. 791. In the first part of the survey, NERC requested that participants respond to the following questions:

[18] Reliability Standard CIP-002-5.1 is the first step in applying the protections of the CIP version 5 standards, requiring responsible entities to identify their high and medium impact BES Cyber Systems and their assets containing low impact BES Cyber Systems.

[19] Initially, NERC staff proposed to issue a data request under Section 1600 of the NERC Rules of Procedure to all registered entities to require their participation in the survey. Based on stakeholder comments on that proposal, however, NERC recognized that many entities were in the initial stages of developing their processes for implementing the CIP version 5 standards and were not in a position to implement such processes to provide NERC meaningful information in the necessary timeframe.

1. Please describe the process you are using to determine which Cyber Assets meet the 15-minute parameter.

2. Please describe any challenges or common problem areas you have encountered in determining whether a Cyber Asset is a BES Cyber Asset.

3. Are there any systems or network components that you have categorically excluded from the scope of the CIP standards due to the definition of BES Cyber Asset? Are these systems or network components programmable? Have you concluded that these systems or networks can never have a real-time impact to the BES under the 15-minute parameter? Please describe the characteristics of these systems and networks.

In the second part of the survey, NERC requested specific information on the types and functions of Cyber Assets that entities are designating as BES Cyber Assets. Specifically, NERC requested that participants complete tables listing the common types of Cyber Assets located at control centers, Transmission stations and substations, and generation plants that could potentially meet the definition of BES Cyber Asset. For each type of Cyber Asset, NERC instructed entities to:

- identify whether the entity has that particular type of Cyber Asset at any of its control centers, Transmission stations/substation or generation plants;

- identify whether all, some, or none of each type of Cyber Asset are designated as BES Cyber Assets; and

- provide the rationale for identifying all, some, or none of such Cyber Assets as BES Cyber Assets.

The purpose of the table approach was to: (1) facilitate responses by listing the common types of Cyber Assets that could potentially be considered BES Cyber Assets; and (2) enable NERC to analyze the manner in which the Implementation Study participants viewed a common set of Cyber Asset types. NERC provided a description of the listed Cyber Asset types and examples of their functional uses in Attachment 1 to the survey for reference by the Implementation Study participants.

Lastly, the survey requested entities to identify and describe whether they have any other Cyber Assets that control Bulk Electric System Elements outside of control centers, Transmission stations or substations, and generation plants, and explain whether such Cyber Assets meet the definition of BES Cyber Asset.

IV. SURVEY RESULTS

a. Process for Determining which Cyber Assets Fall Within the BES Cyber Asset Definition

Each of the Implementation Study participants has a documented process for identifying their BES Cyber Assets pursuant to Reliability Standard CIP-002-5.1. The documentation varied in its level of detail, with some participants, typically the larger entities, including detailed flowcharts with descriptions of the decision points, while others, typically the smaller entities, using a series of questions as filters.[20] As discussed below, while no two entities used the exact same process for identifying BES Cyber Assets, the following fundamental steps were present in each process:

1. Identification of BES Facilities subject to the CIP Reliability Standards.
2. Identification of Cyber Assets at those BES Facilities that perform, or support the performance of, a BES reliability function.
3. Analysis of the real-time (or 15-minute) impact of those Cyber Assets that perform, or support the performance of, a BES reliability function.[21]

Although the various participants had different processes suited to the needs and characteristics of their organization, every Implementation Study participant used a top-down

[20] The CIP version 5 standards do not prescribe a specific process for identifying and categorizing their BES Cyber Systems. The entity has the discretion to develop a process that best suits its needs and results in compliance with the CIP version 5 standards.

[21] Following the identification of BES Cyber Assets, the Implementation Study participants processes then included steps for the grouping of BES Cyber Assets into BES Cyber Systems and, ultimately, the categorization of those systems as high, medium, or low impact according to CIP-002-5.1.

approach to identify their BES Cyber Assets. Specifically, each entity started by compiling a list of their BES Facilities (e.g., Transmission stations/substation, generating plants, and control centers). As part of this step, entities had a "triage" phase designed to eliminate from further consideration any Cyber Assets located at (or associated with) facilities that are outside the scope of the CIP version 5 standards (e.g., those facilities that do not meet the definition of Bulk Electric System). For example, a line-distance protection relay protecting a 230 kV Transmission Facility would be subject to further analysis, while the same type of line-distance protection relay protecting a 69 kV distribution facility would not be included.

Following the identification of their BES Facilities, the participants then identified the Cyber Assets at those Facilities that performed BES reliability functions. The participants generally took one of two approaches to identify these Cyber Assets. In some cases, participants used a function-oriented approach, first reviewing the real-time, reliability-based functions carried out at each BES Facility, and then generating a list of the Cyber Assets used to support or perform those functions. Under this approach, participants further analyzed the Cyber Assets that were used to support or perform the reliability-based functions to determine whether they met the timing element of the BES Cyber Asset definition. In others cases, participants used an asset-oriented approach, starting with an identification of the Cyber Assets (or type of Cyber Assets) at each of the locations followed by an analysis of the functions performed by those Cyber Assets. If those functions were reliability-based, then the participant further analyzed the Cyber Assets to determine whether they met the timing element of the BES Cyber Asset definition.

As noted, under either approach, entities had to determine whether a Cyber Asset performed, or supported the performance of, a reliability-based function. To help identify the relevant BES reliability functions, the Implementation Study participants reported that they started

by either reviewing the NERC Functional Model or using the concept of BES reliability operating services ("BROS"), which is discussed in the Guidelines and Technical Basis section of Reliability Standard CIP-002-5.1. In making this identification, the participants looked at: (1) the reliability functions associated with the type of Facility at which the Cyber Asset was located or associated with;[22] and (2) the reliability functions associated with the functional registration of the participants (e.g., if an entity was registered as a Reliability Coordinator, then Reliability Coordinator functions were analyzed at their control centers).

While there were some deviations in the manner in which the Implementation Study participants determined whether the Cyber Asset performed, or supported the performance of, a reliability-based function, each of the participants essentially analyzed whether the loss, degradation, or misuse of a Cyber Asset could result in: (1) a direct impact to a BES Facility by tripping, failing to trip, or derating that Facility; or (2) any other adverse reliability impact at the Facility. After answering these types of questions, the entities ultimately developed a list of Cyber Assets (or types of Cyber Assets) used to perform, or support the performance of, BES reliability functions at their BES Facilities subject to the CIP Reliability Standards. If a Cyber Asset was not on the list, it was deemed not to be a BES Cyber Asset. If, however, a Cyber Asset was on the list because it performed, or supported the performance of, a reliability-based function, the participants went on to analyze whether the Cyber Asset satisfied the timing component of the definition (i.e., whether the impact of the loss, misuse, or degradation of the Cyber Asset occurred within 15-minutes of its required operation, misoperation, or non-operation).

[22] For example, only transmission-related functions were analyzed for Cyber Assets associated with Transmission stations/substation, and generation-related functions were analyzed for control systems inside of generating plants. Depending on the functions performed at control centers, entities looked either transmission functions, generation functions or both.

The implementation Study participants reported that the 15-minute parameter did not present much ambiguity. The Implementation Study participants found that, if a Cyber Asset performed, or supported the performance of, a BES reliability function, any adverse impact resulting from the loss, misuse or degradation of that Cyber Asset would occur in significantly less time than 15 minutes (e.g., milliseconds to tens of seconds) of its required operation, misoperation, or non-operation, or a significantly longer time than 15 minutes (e.g., hours to days). As one participant stated:

> In general, the 15-minute parameter did not matter when considering the loss of the Cyber Asset and its adverse impact to the BES. The adverse impact could be determined upon immediate loss of the Cyber Asset.

For example, entities often configure line-distance protection systems to operate automatically, without human interaction, often in under one second, to open lines in response to a fault. So if a particular line protection relay was configured to open and close circuit breakers at a BES Facility, the timing element was clearly met because the impact of the misoperation or non-operation of that relay would occur almost immediately. Similarly, SCADA systems at control centers used during real-time operations clearly meet the 15-minute parameter. These system are used to gather data from the field, process it (e.g., limit checking, alarm generation, and database storage), and use the processed data to make real-time decisions (either through autonomous supervisory control decisions, such as AGC, or operator-initiated supervisory control actions, such as breaker control).

In contrast, a digital fault recorder at Transmission stations used to record (often at millisecond resolution) the electrical characteristics of a transmission line for after-the-fact, off-line engineering analysis, sometimes days later, would not satisfy the 15-minute parameter. Only if the system operator analyzed the recorded values for use in real-time operations would such digital fault recorders be deemed BES Cyber Assets. Similarly, participants reported that Cyber

Assets at coal-fired generating plants that control the movement of the coal from the fuel pile into the hopper to be pulverized and fed into the boiler to power the plant would not have a 15-minute impact. That is because, while the boiler continuously needs fuel to keep the plant running, plant designs typically use a fuel hopper that can store several hours' worth of coal, and plant procedures typically require that the hopper be continuously kept nearly full. Because the plant can continue to operate for several hours with the coal in the hopper, the Cyber Asset controlling the movement of the coal into the hopper does not have a 15-minute impact (although the Cyber Assets moving coal out of the hopper to be processed for burning do have a 15-minute impact, and would be BES Cyber Assets).[23]

One of the Implementation Study participants created efficiencies in its process by developing and maintaining a "catalog" of Cyber Assets that allowed them to perform and document the impact analysis once and re-use it at similar locations. This approach was most beneficial in the transmission environment, where many hundreds or thousands of Cyber Assets performing the same function are installed at large numbers of Transmission stations or substations. For example, a particular entity may have thousands of line-distance protection relays that all perform the same reliability function and have the same timing characteristics. By performing the analysis once and referring to it during the analysis of other locations, the entity's process was more efficient and produced consistent results.

[23] As explained below, although a Cyber Asset that does not have real-time impact, such as a fault recorder, need not be protected as a BES Cyber Asset under the CIP version 5 standards, this does not mean that the Cyber Asset does not require some level of protection. Depending on network configurations, the Cyber Asset may qualify as a Protected Cyber Asset, an Electronic Access Control or Monitoring System, or a Physical Access Control System such that certain protections will be required. Further, entities are likely to voluntarily apply some protections to Cyber Assets that are not subject to any protections under the CIP version 5 standards to ensure their systems continue to operate effectively and efficiently. The CIP Reliability Standards, however, are designed to focus industry resources on protecting those Cyber Assets with real-time impact.

As noted above, on the whole, the implementation of these processes resulted in the identification of BES Cyber Assets consistent with the language and intent of the CIP version 5 standards as well as NERC's expectations. Nevertheless, NERC identified areas for improvement. First, in a few of cases, Implementation Study participants used different processes for identifying BES Cyber Assets at different types of BES Facilities (i.e., one process for transmission facilities, one process for generation facilities, and another process at control centers). While entities have the flexibility under the CIP version 5 standards to use different processes for different types of Facilities based on their organizational needs, entities should take care to ensure that each of these processes include all of the necessary factors. In at least one instance, an Implementation Study participants process for analyzing Cyber Assets at control centers included how the entity would consider the misuse of Cyber Assets but its process for transmission and generation facilities did not specifically include such a step. Where an entity uses more than one process, it is important to compare and contrast those processes to make sure that the various business units develop processes that cover all the necessary steps.

Additionally, NERC noted that the less detailed procedures could benefit from additional documentation and formalization of procedures, including the use of flowcharts or similar process flow documents, to help ensure that all decision paths are accounted for when applying the procedure.

NERC is working with the Regional Entities and the Implementation Study participants to develop guidance to share lessons learned with industry regarding best practices for identifying BES Cyber Assets.

b. Challenges and Common Problem Areas in Designating BES Cyber Assets

Although the survey results indicate that the BES Cyber Asset definition is sound, the survey results also highlight particular areas that require additional clarification and guidance to

help ensure that responsible entities are properly and consistently applying the BES Cyber Asset definition. As part of the survey, NERC requested that the Implementation Study participants identify any challenges or common problem areas they encountered in determining whether a Cyber Asset is a BES Cyber Asset. Based on the results of the survey, NERC also identified certain areas that could lead to the improper designation of BES Cyber Assets. The following is a description of the challenges and common problem areas that the Implementation Study participants and NERC identified:

- *Meaning of "Programmable Electronic Device"* – Before an entity determines whether a device is a BES Cyber Asset, it must first determine whether the device is a Cyber Asset, which is defined as a "programmable electronic device[], including the hardware, software, and data in those devices." A number of entities stated that an initial challenge to identifying BES Cyber Assets was determine whether a device is programmable, which is not a defined term in the NERC Glossary.

- *Application of the terms "unavailable," "degraded," and "misused"* – A few participants stated that it was unclear exactly how to apply the term "misuse." NERC also noted that there were some inconsistencies in how certain participants applied that term to their various types of Cyber Assets. Further, while the differences were slight, there were some inconsistencies in how the Implementation Study participants viewed the terms "unavailable" and "degraded."

- *Meaning of the phrases "Adverse Impact" and "Reliable Operations"* – Based on the survey results, there were some inconsistencies in what entities considered to be adverse impact on reliable operations. One entity stated that these terms "mean different things to different people" and lead to prolonged discussions of the level and type of reliability impacts that need to be considered under the definition.

- *Meaning of the Phrase "When Needed"* – The BES Cyber Asset definition looks at the reliability impact on a BES Facility, system or equipment when that Facility, system, or equipment is needed. Based on the results of the survey, it appears that there was some confusion as to the circumstances under which that impact should be measured. One participant pointed out that clarification on the contingencies that should be considered would provide for greater consistency in application of the BES Cyber Asset definition.

- *Situational Awareness* – The survey results revealed that there was some inconsistency in how Implementation Study participants evaluated Cyber Assets that performed or supported situational awareness at control centers. At least one entity stated that it was a challenge to determine when a situational awareness device could have an impact on real-time operations and, consequently, should be identified as a BES Cyber Asset.

- *Evidence for Determinations* – One Implementation Study participant noted that because a determination of whether a Cyber Asset is a BES Cyber Asset often depends on the judgment of a subject matter expert, the type of documentation or evidence necessary to demonstrate the validity of the decision to an auditor is unclear.

- *Resource Requirements* – A number of participants highlighted that the resource requirements for making these determinations is significant. Participants noted that because a determination depends on the function of a particular Cyber Asset, not just the type of Cyber Asset, it requires significant time and effort given the multitude of assets that serve many different functions. One participant noted that it was a challenge to look at each Cyber Asset in depth, in part, because the entity needs to rely on subject matter experts that are not necessarily familiar with the CIP Reliability Standards and cyber issues more generally.

- *Redundancy* – One participant noted that the inability to consider redundancy was a challenge because it led to the identification of significantly more BES Cyber Assets than would otherwise be required if redundancy could be considered.

NERC is currently working with the Implementation Study participants and the Regional Entities to discuss these issues and provide guidance to the broader stakeholder community, through various mechanisms, including guidance documents, training workshops, and other targeted outreach efforts, as appropriate.[24] Notably, Implementation Study participants did not identify the application of the 15-minute parameter as a challenge in properly identifying BES Cyber Assets. Rather, as discussed above, the participants indicated it was a relatively straightforward determination once it understood the reliability function performed by the Cyber Asset and the potential impact of the Cyber Asset if it was unavailable, misused or degraded.

NERC notes that, consistent with the BES Cyber Asset definition, entities cannot consider redundancy when determining whether a Cyber Asset meets the definition. Redundancy is useful in achieving availability of a system accounting for "natural" failures, such as hardware failures and testing of new software in a live environment where only one of a set of redundant systems is upgraded. Further, redundancy cannot be used as a basis for assessing the impact of a Cyber Asset

[24] For example, a guidance document on the meaning of the phrase "programmable electronic device" is posted on NERC's website for industry comment at this time.

because: (1) a malicious attacker could modify multiple Cyber Assets in a redundant configuration almost as easily as he could affect a single system; and (2) the impact of a Cyber Asset must be analyzed under the BES Cyber Asset definition for *all* possible configurations, including the failure of one of a set of redundant Cyber Assets, which would reduce the redundant system to a non-redundant system.

c. Types or Functions of Cyber Assets Excluded from the Definition of BES Cyber Asset

As described above, to better understand the types and functions of Cyber Assets that would be included or excluded under the BES Cyber Asset definition, NERC requested that participants complete tables listing the common types of Cyber Assets located at control centers, Transmission stations and substations, and generation plants to: (1) identify whether the entity has that particular type of Cyber Asset at any of its control centers, transmission stations/substation or generation plants; (2) identify whether all, some, or none of each type of Cyber Asset are designated as BES Cyber Assets; and (3) provide the rationale for including or excluding all, some, or none of such Cyber Assets from designation as BES Cyber Assets. Exhibit 2 to this informational filing provides a detailed summary of the survey responses for each type of Cyber Asset listed in the tables, showing the types and functions of Cyber Assets the Implementation Study participants included or excluded under the BES Cyber Asset definition and the rationale as to why.

In brief, as is evident from the aggregated responses included in Exhibit 2, there was, overall, consistency across the Implementation Study participants in the types of Cyber Assets identified as BES Cyber Assets and the reasons for including or excluding a particular Cyber Asset. The survey shows that a determination of whether a particular Cyber Asset is a BES Cyber Asset is dependent on the function performed by that Cyber Asset and whether that function is integral

to real-time operations. To be clear, while there are certain core systems – such as EMS/SCADA, AGC, DCS, relays, and RTUs – that ordinarily support real-time reliability functions and are generally understood to be BES Cyber Systems, entities must still evaluate the functionality of those systems to determine whether the Cyber Assets that comprise those systems would be considered BES Cyber Assets. Further, an entity can have multiples of the same type of Cyber Asset at a given location or spanning multiple locations, some of which are components of a reliability-based system while the others simply support a general corporate function. Simply looking at the asset type is not determinative; instead, entities must evaluate how the particular Cyber Asset is used, the functions it is performing, the BES elements it is supporting, etc.

In many instances, the Implementation Study participants reported that, based on their factual analysis, some, but not all, of a Cyber Asset type were designated as BES Cyber Assets, depending on the function and use of a particular Cyber Asset. For example, there are numerous intelligent electric devices ("IEDs") at any given Transmission station or substation (e.g., digital relays). Some of those IEDs operate BES equipment, such as switches or breakers, and could have an immediate impact on the BES. Other IEDs are used strictly for capturing data for use in future, "after the fact" diagnostic efforts (like digital fault recorders) and have no real-time impact. The former would be BES Cyber Assets, the latter would not BES Cyber Assets.

As another example, Implementation Study participants reported that in the generation plant context, the classification of programmable logic controllers ("PLCs"), which are generic process controllers, depends on the impact of the particular process they are controlling. For example, a PLC used to bring coal into the generation plant from the coal yard would likely not be a BES Cyber Asset because plants usually have eight hours or more of coal their hoppers such that the unavailability, degradation, or misuse of that PLC is not going to affect the reliable operation

of the generators in 15 minutes or less. Water chemistry PLCs are similar in that they are providing water into storage tanks and the process pulls water from the tanks as needed but there is no 15-minute impact to generation resulting from the loss, degradation, or misuse of those PLCs. In contrast, a PLC at a hydroelectric generating unit that is directly controlling the gates would be a BES Cyber Asset because the loss, misuse, or degradation of that PLC could have an immediate impact on the reliable operation of the hydroelectric facility.

The most common reasons why a Cyber Asset was excluded from the BES Cyber Asset definition were:

1. The Cyber Asset supported a non-BES Facility, system, or set of equipment (e.g., a line protection relay for a distribution line).
2. The Cyber Asser did not support a reliability function (e.g., a meter used only for billing or local readout functions as opposed to providing data to an EMS).
3. The Cyber Asset, while used to support BES functions, did not have operational impact (e.g., a fault recorder at a Transmission station used to record operational data for "after the fact" analysis of an event).

As shown in Exhibit 2, the Implementation Study participants frequently identified the following devices or systems as having no reliability function and/or ability to adversely impact the BES within a 15-minute time horizon: economic dispatch optimization systems; printers; historians; fault recorders; revenue meter information collection systems; day-ahead planning systems; and long term load forecasting systems.

Importantly, however, while entities may not designate a particular Cyber Asset as a BES Cyber Asset under certain circumstances, the Cyber Asset may be subject to protections under the CIP version 5 standards if it meets the definition of a Protected Cyber Asset ("PCA"), Electronic Access Control or Monitoring System ("EACMS"), or a Physical Access Control System ("PACS"). These terms are defined in the NERC Glossary as follows:

- *PCAs* – "One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter."

- *EACMS* – "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems."

- *PACS* – "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers."

Under the CIP version 5 standards, PCAs are afforded almost the same protections as the BES Cyber Systems with which they are associated. Accordingly, while a network printer or a historian at a control center, for instance, may not perform a reliability function or meet the 15-minute parameter, entities may be required to protect those devices under the CIP version 5 standards if those devices are in an ESP. This ensures, for instance, that printers and historians on the same network as BES Cyber Systems could not be used as vehicles to perpetrate a cyber-attack against a BES Cyber System. Similarly, Cyber Assets that provide electronic or physical access controls would be protected under the CIP version 5 standards because protecting such Cyber Assets is necessary for protecting BES Cyber Systems.

On the whole, the responses to the survey were consistent with NERC's expectations and the intent and language of the BES Cyber Asset definition. As noted above, however, one of the areas that needs additional focus is how to classify Cyber Assets at control centers that provide situational awareness. Many of the Implementation Study participants excluded certain situational awareness devices from the BES Cyber Asset definition. Implementation Study participants indicated that map-boards, for instance, need not be designated as BES Cyber Assets because they have no control capability and are often used only for next business day restoration criteria or serve as a secondary source of information. In other cases, certain Implementation Participants indicated that it was a challenge to determine when a situational awareness device could have an impact on

real-time operations. NERC, the Regional Entities and the Implementation Study participants are working together to better understand how situational awareness devices are used in control centers and under what circumstances they could have a 15-minute impact if relied upon by system operators in carrying out their real-time obligations.

d. Regional Entity Feedback

Consistent with the directive in Order No. 791, the following section provides feedback from the Regional Entities that participated in the Implementation Study on lessons learned with the application of the BES Cyber Asset definition. Based on their experiences during the Implementation Study, the Regional Entities agreed that the 15-minute parameter need not be modified to ensure entities properly and consistently identify BES Cyber Assets. The Regional Entities found that a Cyber Asset in a control center, Transmission station/substation, or generating plant typically operates in a sub-second time frame or clearly has no impact within the 15-minute window. Although none of the Regional Entities reported an instance where a Cyber Asset's impact was near the 15-minute threshold, the Regional Entities stated that, if it were close, an entity would need to submit documented evidence to justify its classification. Nonetheless, the Regional Entities noted that the 15-minute impact determination is a relatively clear binary decision as to whether a Cyber Asset is included or excluded under the BES Cyber Asset definition.

While the Regional Entities did not find that the 15-minute parameter presented significant difficulties in applying the BES Cyber Asset definition, they did point to other components of the definition that could benefit from additional clarification and guidance. Many of these components overlap with the challenges and problem areas identified above in Section III of this informational filing. In particular, two Regional Entities noted a need to provide additional clarification on the application of the phrase "when needed." The Regional Entities noted that absent further clarification, responsible entities may interpret this phrase to allow the exclusion of Cyber Assets

from the BES Cyber Asset definition if engineering studies can demonstrate the Cyber Asset is not needed or if redundant assets support the loss of that Cyber Asset. The Regional Entities noted that engineering studies cannot factor in every contingency, and redundant assets do not negate the "when needed" phrase under the BES Cyber Asset definition. The Regional Entities stated that the issuance of additional guidance on the meaning and intent of the phrase "when needed" could help avoid the improper application of the BES Cyber Asset definition.

A number of Regional Entities also noted that the phrase "adverse impact" could benefit from additional clarification. One Regional Entity noted that during the Implementation Study there was significant discussion about how to exactly apply this phrase, with some taking a more narrow approach and others taking a broader approach. For instance, there were questions as to how to treat a Cyber Asset that, if compromised, may not have a meaningful impact on reliable operation of the BES as a whole but may impact the reliable operation of one or more BES Facilities, systems, or equipment. The Regional Entities stated that responsible entities need further guidance on the level and types of impact to consider when determining whether a Cyber Asset is a BES Cyber Asset.

Similarly, one Regional Entity noted that while the definition requires entities to look at the adverse impact of Cyber Assets on "one or more Facilities, systems, or equipment," the terms "systems" and "equipment" are not defined in the NERC Glossary. The Regional Entity expressed that additional explanation of the terms "systems" and "equipment" would help responsible entities identify BES Cyber Assets.

In addition to clarification on terms used the BES Cyber Asset definition, some Regional Entities also stated that the phrase "programmable electronic device" in the Cyber Asset definition could benefit from clarification. In particular, Regional Entities noted that entities asked whether

a programmable electronic device included only those devices with a microprocessor or include any configurable device.

Aside from the feedback to clarify undefined terms, a Regional Entity stated that, although this was not an issue for any particular Implementation Study participant, entities need to understand that the BES Cyber Asset definition does not require routable protocol connectivity. Therefore, the Regional Entity stated, Cyber Assets not connected to a network via a routable protocol and not required to be within an ESP still need to be evaluated to determine if they meet the BES Cyber Asset definition.

NERC is working with the Regional Entities and the Implementation Study participants to consider this feedback and share lessons learned from the Implementation Study and the survey with the broader stakeholder community. NERC understands the need for consistent understanding of the CIP Version 5 standards across the ERO in order for entities to effectively transition to CIP Version 5 compliance.

V. CONCLUSION

For the reasons set forth above, NERC respectfully requests that the Commission accept this informational filing as compliant with the Commission's directive in Order No. 791.

Respectfully submitted,

/s/ Shamai Elstein
Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 3, 2015

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 3rd day of February, 2015.

/s/ Shamai Elstein

Shamai Elstein

Counsel for the North American Electric Reliability Corporation

EXHIBIT 1

BES Cyber Asset Survey

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Survey Regarding the Scope of the Term "BES Cyber Asset" for Participants in the Implementation Study for the CIP V5 Transition Program

RELIABILITY | ACCOUNTABILITY




Introduction and Survey Scope

The North American Electric Reliability Corporation ("NERC") requests that the participants in the Implementation Study for the CIP Version 5 Transition Program (the "Implementation Study") provide NERC certain data and information (the "Survey") regarding the scope of the term "BES Cyber Asset," as defined in NERC's *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"). NERC requests that participants complete the Survey by **November 7, 2014** and email it to Marisa Hecht at Marisa.Hecht@nerc.net and Shamai Elstein at shamai.elstein@nerc.net.

The purpose of the Survey is work with the Implementation Study participants to respond to FERC's directive from Order No. 791[1] to conduct a survey regarding the scope of the NERC Glossary term "BES Cyber Asset" and submit an informational filing based on the data collected. In Order No. 791, FERC approved new and modified Critical Infrastructure Protection ("CIP") Reliability Standards, collectively referred to as the CIP Version 5 Standards, as well as new and modified terms to be incorporated into the NERC Glossary. Among others, FERC approved the following definition for the NERC Glossary term "BES Cyber Asset":

> A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.

To better understand the scope and reach of the term "BES Cyber Asset," the Commission directed NERC to conduct a survey of responsible entities during the implementation period for the CIP Version 5 Reliability Standards to determine the types of Cyber Assets that are included or excluded under the definition of BES Cyber Asset.[2] Based on the data obtained from the survey, the Commission further directed NERC to explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15-minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition.[3] In Order No. 791-A, the Commission clarified that NERC could use the participants in the Implementation Study as the basis for the survey.

---

1 *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013).

2 Order No. 791 at PP 123-125.

3 Order No. 791 at P 124.

FERC directed NERC to submit the informational filing within one year of the effective date of Order No. 791, which is February 3, 2015. The Survey is designed to satisfy the Commission's directive to conduct a survey of responsible entities on the scope of the term "BES Cyber Asset" and to collect data necessary for the informational filing.

Understanding the scope and reach of the term "BES Cyber Asset" is an important step in ensuring that entities are properly and consistently determining the types of Cyber Assets that are included or excluded under the definition of BES Cyber Asset. The Survey consists of two parts:

(1) Participants are requested to describe (1) their process for determining which Cyber Assets meet the 15 minute parameter, and (2) challenges they have faced or common problem areas they identified during the Implementation Study.

(2) Participants are then asked to describe the types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why.

Survey

PART 1 - Process for Identifying BES Cyber Assets

a. Please describe the process you are using to determine which Cyber Assets meet the 15 minute parameter.

_____

_____

_____

b. Please also describe any challenges or common problem areas you have encountered with respect to determining whether a Cyber Asset is a BES Cyber Asset.

_____

_____

_____

c. Are there any systems or network components that you have categorically excluded from the scope of the CIP standards due to the definition of BES Cyber Asset? Are these systems or network components programmable? Have you concluded that these systems or networks can never have a real-time impact to the BES under the 15-minute parameter? Please describe the characteristics of these systems and networks.

_____

_____

_____

PART 2: Types of Cyber Assets Included or Excluded from Designation as a BES Cyber Asset

a. Pleased describe the types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets, and the rationale as to why, by completing the tables below.

The purpose of the table approach is to: (1) facilitate your responses to FERC's questions by listing the common types of Cyber Assets located at control centers, Transmission stations and substations, and generation plants that could potentially be considered BES Cyber Assets, and (2) help ensure that NERC can understand how a common set of Cyber Asset types are viewed across the six Implementation Study participants. For an explanation of the listed Cyber Assets and examples of their functional uses, please refer to Attachment 1 hereto.

I. ***Control Centers:***

Type of Cyber Asset	**Please provide the following information for each type of Cyber Asset listed below:** **(1) Identify whether you have such Cyber Assets at your control centers.** **(2) Identify whether all, some, or none of each type of Cyber Asset are designated as a BES Cyber Asset.** **(3) Provide the rationale for including or excluding the type of Cyber Asset from designation as a BES Cyber Asset. If a type of Cyber Asset would be included under some circumstances and excluded under others, please explain.**
Application Servers	
Data Servers	
HMI Workstations	
Network Printer	
Data Acquisition	
Data interchange	
PDC	
Computer Networking	
Communications Processing	
Diagnostic	
Fault Recorder	
Historian	

Situational Awareness	
Precision Time Device	
Training Simulator	
Development & Testing	
Infrastructure Support	
Marketing Systems	
Other	

II. ***Transmission Station / Substation:***

Type of Cyber Asset	**Please provide the following information for each type of Cyber Asset listed below:** **(1) Identify whether you have such Cyber Assets at your Transmission stations and substations.** **(2) Identify whether all, some, or none of each type of Cyber Asset are designated as a BES Cyber Asset.** **(3) Provide the rationale for including or excluding the type of Cyber Asset from designation as a BES Cyber Asset. If a type of Cyber Asset would be included under some circumstances and excluded under others, please explain.**
IED / Protective Relay	
RTU	
Controller (PLC)	
Data Concentrator	
Meter / indicator	
Intelligent instrumentation	
Tap Changer	
HMI Workstation	
Network Printer	
Computer Networking	
Communications Processing	

Equipment Diagnostic / Maintenance	
Fault Recorder	
PMU	
PDC	
Historian	
Precision Time Device	
Development & Testing	
Infrastructure Support	
Other	

III. *Generation Plants:*

Type of Cyber Asset	**Please provide the following information for each type of Cyber Asset listed below:** **(1) Identify whether you have such Cyber Assets at your generation plants.** **(2) Identify whether all, some, or none of each type of Cyber Asset are designated as a BES Cyber Asset.** **(3) Provide the rationale for including or excluding the type of Cyber Asset from designation as a BES Cyber Asset. If a type of Cyber Asset would be included under some circumstances and excluded under others, please explain.**
Controller (PLC)	
Distributed Control System (DCS)	
Sensor / Actuator / Transmitter	
Meter / Indicator	
HMI Workstation	
Application Server	
Network Printer	
Data Server	
Historian	
Computer Networking	

Equipment Diagnostic / Maintenance	
Fault Recorder	
IED / Relay	
RTU	
PMU	
PDC	
Precision Time Device	
Development & Testing	
Infrastructure Support	
Other	

b. Other Locations**:** If you have any other Cyber Assets that control BES Elements outside of control centers, Transmission stations or substations, and generation plants, please describe their location and function, and explain whether they meet the definition of BES Cyber Asset.

_____

_____

_____

_____

_____

NERC Contact Information

If you have any questions regarding this Survey, please contact Scott Mix, CIP Technical Manager, Critical Infrastructure Department, at 215-853-8204 or by e-mail at Scott.Mix@nerc.net.

Alternate NERC Point(s) of Contact:

Nicholas Santora
CIP Cybersecurity Specialist
Critical Infrastructure Division
404.446.9690
Nicholas.Santora@nerc.net

Felek Abbas
CIP Compliance Auditor, CIP & Operations Assurance
202-400-3017
Felek.Abbas@nerc.net

Marisa Hecht
Standards Developer, Standards
404-446-9620
Marisa.Hecht@nerc.net

Ryan Stewart
Standards Developer, Standards
202-844-8091
Ryan.Stewart@nerc.net

Shamai Elstein
Counsel
202-400-3009
Shamai.elstein@nerc.net

ATTACHMENT 1

Explanation and Functional Uses of Asset Types

The following is a description of the Cyber Assets commonly installed and used at control centers, Transmission stations or substations, or generation plants. The Cyber Assets listed here include BES Cyber Assets, as well as support systems and Electronic Control and monitoring Systems (EACMS) and Physical Access Control Systems (PACS).

Many of the Cyber Assets described below perform multiple functions. When responding to the survey, only account for each Cyber Asset once, picking the most applicable function performed by the Cyber Asset.

1. Control Center

- **Application Server**: Traditional computer used for executing Bulk Electric System operations applications such as status monitoring, limit checking, alarm generation, log management, automatic generation control (AGC), economic dispatch, interchange scheduling, unit scheduling, state estimation, contingency analysis, power flow analysis, switching studies, etc.
- **Data Server:** Similar to an application server, but primarily used to provide data to application servers. Data servers include "traditional" servers running database software with locally attached storage, as well as network-attached storage servers (disk servers).
- **HMI (Human Machine Interface) Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human grid operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Data Acquisition Server**: Communications front-end processors used to communicate to other computer sites, control centers, field devices, or generation plants by receiving data from remote sites, process the data into local format, and store it for local use. Some data acquisition servers contain specialized hardware used to communicate to field devices; other data acquisition servers receive data via computer network connections.
- **Data Interchange**: Communications servers (e.g. ICCP servers) used to communicate intersite data between control centers and other facilities that serve a BES function.
- **Phasor Data Concentrator (PDC)**: A device that manages data feeds from multiple Phasor Measurement Units (PMUs).

- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, security event and incident management systems, EACMS, etc.
- **Communications Processing Devices**: Devices used to perform protocol conversions, encapsulate serial data into a routable protocol, encrypt communications, etc.
- **Diagnostic Devices**: Devices used to troubleshoot hardware or software; at a control center diagnostic devices are most often attached to the local area network but could be attached to other Cyber Assets. Diagnostic devices can be normal Cyber Assets such as laptop computers or specialized diagnostic equipment.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the Transmission elements for after-the-fact analysis.
- **Historian**: Generally, a combination of computer server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Situational Awareness**: Systems used to provide situational awareness in a real-time Bulk Electric System operations environment (e.g. video mapboards, tile mapboard controllers, video trending).
- **Precision Time Device:** Device used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Training Simulator**: Computers (including application servers, database servers, HMI) that are used to train operators on various power system operations scenarios, and to test new operational procedures for validity.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, database updates, and power system model changes prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Marketing Systems**: Systems supporting marketing functions that may be located inside ESPs containing BES Cyber Systems. Examples include OASIS calculators, market pricing systems, market clearing systems, market billing systems, etc.

  Other: Any other Cyber Asset not described above. Please specify the application or function.

2. Transmission Station / Substation

- **Intelligent Electronic Device (IED) / Protective Relay**: IED or relay device protection system used to sense fault conditions (e.g., on Transmission lines), and take rapid autonomous actions to isolate the fault to prevent cascading fault conditions or equipment damage
- **Remote Terminal Unit (RTU)**: A device or system used to send telemetry data from the substation to the control center, and to receive control commands from the control center.
- **Programmable Logic Controller (PLC)**: Substation automation device used to coordinate actions taken by multiple IEDs, or when processing capabilities beyond the capability of an IED are required.
- **Data Concentrator**: A device or system used to collect data from multiple IEDs and provide a single data interface to the RTU.
- **Meter / Indicator**: A device used to provide local readout of values (e.g., bus voltage) or indication of status (e.g., breaker open/close). Meters / indicators may also collect and transmit values to other Cyber Assets.
- **Intelligent instrumentation**: Primary instrumentation used to sense values (e.g., voltage, current) or status (e.g., breaker or switch position). Primarily used by IEC 61850 enabled substations.
- **Tap Changer**: A device located on a transformer that allows the transformer winding ratio to be controlled remotely.
- **HMI Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, EACMS etc.
- **Communications Processing Devices**: Devices used to perform protocol conversions, encapsulate serial data into a routable protocol, encrypt communications, etc.
- **Equipment Diagnostic / Maintenance**: Devices used to monitor the behavior of the substation computers, calibrate the instrumentation, or diagnose problems with the control or networking components.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the Transmission elements for after-the-fact analysis.

- **Phasor Measurement Unit** (**PMU)**: A device that performs high-speed monitoring and analysis of voltage and current values and waveforms. In some cases, PMU data is used for after-the-fact analysis; in other cases, PMU data is used for real-time autonomous control.
- **Phasor Data Concentrator** (**PDC)**: A device that manages data feeds from multiple PMUs.
- **Historian**: Generally, a combination of computer server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Precision Time Device:** Device used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, and database updates prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Other**: Any other Cyber Asset not described above. Please specify the application or function.

3. <u>Generation Plants</u>

- **Controller (PLC)**: First level control system, used to coordinate the actions of a specific set of sensors and actuators. Controllers are programmed to take the input of specific sensors, process their data, and send output control commands to actuators, generally with a feedback loop to assess the impact of the control action, and take additional control actions if necessary. Individual controllers send status and values to higher level controllers and application servers for supervisory control and display to operators.
- **Distributed Control System (DCS)**: Modules, processors, communications relays, and other sub-components that control the plant and allow operators at HMI interfaces to manipulate the plant.
- **Sensor / Actuator / Transmitter**: Primary input and output elements in a distributed control system. Sensors sense process values (e.g., pressure, temperature); actuators invoke changes in the process (e.g., open and close valves, change the speed of motors), and transmitters provide the local interface between the sensor and actuator to the control system hardware. Modern sensors and actuators contain embedded transmitters, older sensors and actuators require transmitters to translate analog signals to digital signals, or to allow the analog control signals to travel longer distances.

- **Meter / Indicator**: Device used to provide local readout of values (e.g., pressure, temperature) or indication of status (e.g., valve position). Meters / indicators may also collect and transmit values to other Cyber Assets.
- **HMI Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Application Server**: Traditional computer nodes used for executing Bulk Electric System operations applications such as plant optimization, or to coordinate the action of multiple independent control systems.
- **Data Server**: Similar to an application server, but primarily used to provide data to application servers. Data servers include "traditional" servers running database software with locally attached storage, as well as network-attached storage servers (disk servers).
- **Historian**: Generally, a combination of computer server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, EACMS, etc.
- **Equipment Diagnostic / Maintenance Devices**: Devices used to monitor the behavior of the generation plant computers, calibrate the instrumentation, or diagnose problems with the control or networking components.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the Transmission elements for after-the-fact analysis.
- **Intelligent Electronic Device (IED) / Protective Relay**: IED or relay device protection system used to sense fault conditions (e.g., on a generator bus), and take rapid autonomous actions to isolate the fault to prevent cascading fault conditions or equipment damage.
- **Remote Terminal Unit (RTU):** A device or system used to send telemetry data from the substation to the control center, and to receive control commands from the control center.
- **Phasor Measurement Unit (PMU)**: A device that performs high-speed monitoring and analysis of voltage and current values and waveforms. In some cases, PMU data is used for after-the-fact analysis; in other cases, PMU data is used for real-time autonomous control.

- **Phasor Data Concentrator (PDC):** A device that manages data feeds from multiple PMUs.
- **Precision Time Device:** Device used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, and database updates prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Other**: Any other Cyber Asset not described above. Please specify the application or function.

EXHIBIT 2

Types and Functions of Cyber Assets Included or Excluded from Designation as a BES Cyber Asset

Types and Functions of Cyber Assets
Included or Excluded from Designation as a BES Cyber Asset

In Order No. 791, to better understand the scope of the definition of BES Cyber Asset, the Commission directed NERC to conduct a survey of Cyber Assets that are included or excluded under the definition, particularly as a result of the application of the 15-minute parameter. Based on the results of the survey, the Commission required NERC to submit an informational filing explaining, among other things, types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why. The following tables list Cyber Assets commonly installed and used at control centers, transmission stations or substations, or generation plants and provides a summary of survey results for each of these Cyber Assets, explaining whether entities designated some, all or none of these Cyber Assets as BES Cyber Assets and the rationale underlying those designations. Attached hereto is a description of the listed Cyber Asset types and examples of their functional uses.

I. *Control Centers:*

Type of Cyber Asset	Aggregated Survey Responses
Application Servers	All of the survey participants reported that they have designated some or all of their application servers at control centers as BES Cyber Assets. The participants reported that they classified application servers as BES Cyber Assets where such devices supported the operation of SCADA/EMS, which perform a real-time reliability function. Where survey participants indicated that they had application servers that they did not designate as BES Cyber Assets, they explained that such application servers provide functions or support equipment that did not have a real-time reliability impact. For instance, participants noted that application servers are used to only support a historian function, storing historic operating data not used for real-time operations.
Data Servers	All of the survey participants reported that they have designated some or all of their data servers at control centers as BES Cyber Assets. The participants indicated that such data servers are used to support functions necessary for real-time operations, including storing of modeling data and providing information for the SCADA/EMS. Where survey participants indicated that they had application servers that they did not designate as BES Cyber Assets, they explained that that such data servers are not used to support reliability-based or real-time operational functions but, instead, support economic

	dispatch optimization systems, printers, historians, day-ahead planning systems, or long-term forecasting systems.
HMI Workstations	All survey participants identified HMI workstations as BES Cyber Assets. They explained that HMI workstations have direct control over the operation of the BES and, in turn, misuse, degradation, or loss of these HMI workstations would have an adverse impact on the reliable operation of the BES.
Network Printer	None of the survey participants included network printers as BES Cyber Assets. The survey participants stated that network printers do not have an impact to reliability as they do not perform a reliability function and would not affect the reliable operation of the BES within 15 minutes. They serve as printing devices. The survey participants acknowledged, however, that if a network printer is on the same Electronic Security Perimeter (ESP) as a BES Cyber Assets, the network printer would then be identified as a Protected Cyber Asset (PCA) and protected as such.
Data Acquisition	All survey participants indicated that data acquisition devices at control centers should be considered BES Cyber Assets because they collect data used in real-time. Real-time data acquisition is a primary function of EMS systems and the loss, degradation, or misuse of EMS within 15 minutes would affect the reliable operation of the BES. Specifically, the participants identified front end communication servers as BES Cyber Assets because they communicate with RTUs in the field.
Data interchange	All survey participants identified some data interchange devices as BES Cyber Assets. Data interchange servers were classified as BES Cyber Assets where they communicate information used to in real-time operations. For instance, where they communicated information to a Regional Transmission Operator (RTO) that the RTO uses to make operations decisions or where they communicate information between BES Cyber Assets (i.e., Inter Control-center Communications Protocol (ICCP) communications). The survey participants excluded data interchange devices from the BES Cyber Asset definition, however, when such devices are only associated with distribution or development systems.
Phasor Data Concentrator (PDC)	Only one participant indicated that it has a PDC at a control center. That participant explained that the PDC was not a BES Cyber Asset as it had no real-time impact but was used for after-the-fact analysis.
Computer Networking	Survey participants identified those computer networking devices that were within an identified ESP as BES Cyber Assets. The participants concluded that the loss, misuse, or degradation of these devices would have an impact on BES reliability. In particular, many survey participants looked at the misuse clause of BES Cyber Asset to clarify the inclusion of networking devices as BES Cyber Assets. In contrast, computer networking devices that were outside of the ESP, the participants concluded that the misuse of these devices would not cause adverse reliability impact and, in turn, excluded such devices from the definition.
Communications Processing	Survey participants identified communications processing devices as BES Cyber Assets where those devices are used to support EMS. In contrast, survey participants did not identify such devices as BES Cyber Assets where they are used for corporate functions or non-BES elements and, in turn, perform no reliability

	functions and/or do not meet the 15 minute impact rating criteria. Certain survey participants identified that they do not use communications processing devices in their control center.
Diagnostic	None of the survey participants identified diagnostic devices as BES Cyber Assets. A number of survey participants indicated that they did not have such devices at their control centers. For those that did have diagnostic devices at their control centers, they explained that those devices are not used for functions critical to the operation of the BES in real-time but are used for maintenance purposes only.
Fault Recorder	None of the survey participants identified fault recorder devices at their control centers. The survey participants noted that these devices are not typically found in control center environments.
Historian	None of the survey participants identified historians as BES Cyber Assets. They excluded historians from the definition of BES Cyber Asset because they were not used for real-time operations but for historical trending and post-event information only.
Situational Awareness	Only one study participant identified situational awareness devices at control centers as BES Cyber Assets. The other participants excluded Situational Awareness devices, arguing that such devices perform no real-time reliability functions and do not meet the 15-minute parameter. The survey participants excluded "convenience" devices such as map-boards, stating that such devices have no control capability and are used for next business day restoration criteria and/or only serve as a secondary source of information.
Precision Time Device	All survey participants identified their precision time devices and GPS clocks in control centers as BES Cyber Assets. The participants noted that these devices provide time synch for HMO Workstations and servers and, in turn, are critical to the operation of the BES.
Training Simulator	None of the survey participants identified training simulators as BES Cyber Assets. A number of participants stated that they do not have such devices at control centers. For those that had such devices, the participants explained they are not used in real-time operations, that they are on distinct networks outside of an ESP and have no impact to the BES.
Development & Testing	None of the survey participants identified development and testing devices as BES Cyber Assets. The participants stated that either they do not have such devices at control centers or, if they do, they are not used in real-time operations. Rather, they are used for simulation purposes only.
Infrastructure Support	Most survey participants identified certain infrastructure support devices as BES Cyber Assets. Survey participants identified domain controllers hosting DNS for the EMS environment as BES Cyber Asset as well as patch and anti-virus servers as BES Cyber Assets due to their interconnectivity and potential for misuse. In some cases, participants excluded such devices on the grounds the devices perform no reliability function. They noted, however, that such devices would be Electronic Access Control or Monitoring Systems (EACMS) if they performed access control.
Marketing Systems	None of the survey participants identified marketing systems as BES Cyber Assets since they would not affect the reliable operation of the BES.
Other	One participant stated that it had devices, such as EACMS, Physical Access Control Systems (PACS), and corporate PCs, but did not classify such devices as BES Cyber Assets. Another participants noted it had corporate web servers, used for information purposes only, and certain transient devices (e.g., laptop computers) that were not considered BES Cyber Assets.

II. *Transmission Station / Substation:*

Type of Cyber Asset	Aggregated Survey Responses
Intelligent Electronic Devices (IED) / Protective Relay	All survey participants indicated they have some IED / Protective Relay devices identified as BES Cyber Assets. The survey results indicated that such devices were identified as BES Cyber Assets if they protect a BES element or are used to collect real-time data. Survey participants excluded such devices if: (1) the relay was only associated with facilities operating below 100 kV or distribution level facilities, and (2) if the IED collected information used for after-the-fact analysis.
RTU	All survey participants identified some RTUs as BES Cyber Assets. RTUs were included in the BES Cyber Asset if they were associated with Transmission Elements operated at 100 kV or above, interface with other BES Cyber Assets and/or provided situational awareness data about the BES to EMS. RTUs were primary excluded if they were only associated with non-BES facilities or provided data for after-the-fact analysis.
Programmable Logic Controllers (PLC)	Survey participants identified PLCs as BES Cyber Assets if they were used in protective schemes for BES elements. Survey participants excluded PLCs that were not associated with BES elements or could not have a real-time impact. For instance, where the PLC was used (1) in a offline maintenance oil processing facility, (2) for informational relay access alarms, or (3) for monitoring power line carriers.
Data Concentrator	The survey participants identified data concentrator devices as BES Cyber Assets where the data concentrator was used to provide data to the RTU for situational awareness or if the data concentrator functions like an RTU. Survey participants excluded other data concentrators from the BES Cyber Asset definition because they were only used to store data from the transformer monitoring system and, in turn, did not have a 15-minute impact. Additionally, such devices were excluded if they were only associated with transmission elements operated below 100 kV and/or do not interface with other BES Cyber Assets. Certain survey participants indicated they did not have data concentrator devices at their substations
Meter / indicator	Survey participants indicated that meter/indicator devices were considered BES Cyber Assets depending on the voltage level and function of the meter/indicator. Participants included meters/indicators that performed AGC functions because the AGC function is integral to real-time operations. In contrast, devices used for corporate or non-reliability purposes (e.g., billing or a local readout) were excluded from being a BES Cyber Asset. A participant excluded analog meters that are used by the Balancing Authority for control and monitoring because they do not meet the definition of Cyber Asset.

Intelligent Instrumentation	None of the survey participants indicated they had intelligent instrumentation devices at transmission stations/substations.
Tap Changer	Survey participants indicated that tap changer devices were considered BES Cyber Assets where the devices were installed on BES transformers and had the ability to impact and control BES voltages. Participants excluded tap changers where they were associated with non-BES elements. A participant also excluded tap changers that were controlled by the RTU directly and an additional Cyber Asset is not involved in the function of the device.
HMI Workstation	Survey participants identified HMI workstations capable of controlling BES equipment at a transmission stations as BES Cyber Assets. Where the HMI workstation did not have control functionality but were used as an enhancement feature, the participants did not designated them as BES Cyber Assets. Some participants did not identify HMI workstations at their substations.
Network Printer	None of the participants included network printers as BES Cyber Assets. The survey participants stated that network printers do not have an impact to reliability.
Computer Networking	Survey participants classified computer networking devices as BES Cyber Assets where the networking devices were inside of the ESP that control BES Cyber Asset traffic, where they provide connections to RTU functions, or where the device (i.e., router) was used for network connectivity to transfer EMS data to the EMS master. Some survey participants indicated that they had computer networking devices that were classified as EACMS and PACS, not BES Cyber Assets.
Communications Processing	Survey participants classified communications processing devices as BES Cyber Assets where they were used to convert serial data to routable protocol to be delivered to the EMS or provided real-time visibility. In other cases, the survey participants indicated their communication devices did not meet the BES Cyber Asset definition and would have not real-time impact. Other survey participants indicated they had no communications processing devices at transmission substations.
Equipment Diagnostic / Maintenance	None of the study participants identified equipment diagnostic/maintenance devices as BES Cyber Assets. The participants indicated that these devices are used for testing purposes only and not used for real-time operation of the BES.
Fault Recorder	None of the survey participants identified fault recorders as BES Cyber Assets. They indicated that these devices are used for post-event analysis and do not have an impact on the reliability of the BES within 15 minutes.
PMU	Most survey participants indicated that they did not have PMUs at their transmission stations. Those that had PMUs, did not identify them as BES Cyber Assets on the grounds that the PMUs are used for after-the-fact analysis of events, and have no adverse impact on operations in any timeframe.
PDC	None of the survey participants responded that they had PDCs at their transmission stations.
Historian	None of the survey participants classified historians at transmission stations as BES Cyber Assets.

Precision Time Device	None of the survey participants classified precision time devices at transmission stations as BES Cyber Assets. The participants argued that such devices have no adverse impact on reliability and are used for "after the fact" historical data. This post event analysis, although important for sequence of events, will not impact the BES or have an impact within 15 minutes.
Development & Testing	No survey participants indicated that they classified development and testing devices at transmission stations as BES Cyber Assets. These devices were excluded on the grounds that they do not have an impact on reliability of the BES as they are used for simulation only and are used to develop and test changes to BES Cyber Assets prior to putting the device into service at the substation.
Infrastructure Support	None of the survey participants identified infrastructure support as BES Cyber Assets.
Other	One study participant classified transformer monitoring systems as BES Cyber Assets. Another participant identified some BES Cyber Assets that are used to transmit and receive tripping signals from remote locations. Another survey participant identified control relays, digital protective units, pilot relaying units, and transfer trip devices as BES Cyber Assets.

III. *Generation Plants:*

Type of Cyber Asset	Aggregated Survey Responses
Programmable Logic Controller (PLC)	All survey participants identified some PLCs at generating plants as BES Cyber Assets. PLCs were identified as BES Cyber Assets in the following circumstances: (1) the particular PLC can be disturbed and result in a trip or de-rate of a generating unit's output within 15 minutes; (2) the PLC is on a turbine control system (TCS) that can immediately trip a generating unit; and (3) PLCs that function as protection relays that are utilized on various medium and high voltage plant equipment. Participants excluded ash handling system PLCs, water pretreatment PLCs, fuel handling PLCs, and the balance of plant PLCs where the loss or misuse of the PLC that would only affect the unit after many hours or days.
Distributed Control System (DCS)	All survey participants indicated that DCS are BES Cyber Assets. All participants agreed that DCS is critical for the plant to function and the devices controlling the generating units can affect the BES within 15 minutes.
Sensor / Actuator / Transmitter	Survey participants classified some sensors/actuators/transmitters as BES Cyber Assets. The participants explained, however, that it depends on the impact to the generating unit(s) of the particular part of the process that the sensor/transmitter/actuator monitors and controls. Participants identified such devices as BES Cyber Assets if the particular process can be disturbed and result in a trip or de-rate of a generating unit's output within 15 minutes. The impact of individual sensors/transmitters/actuators is considered as part of the system to which it is connected. These devices are the input/output elements from higher level system components (DCS modules, PLCs, etc.) and would for the most part inherit the classification of those higher level components. In contrast, participants explained that sensors for asset management systems, burner management systems, combustion control systems, turbine control systems, turbine water induction protection systems, data acquisition systems, air quality control systems, and waste water treatment systems are not classified as BES Cyber Assets because they cannot affect a generating unit within 15 minutes if misused or degraded.
Meter / Indicator	Survey participants identified meters/indicators as BES Cyber Assets where the devices provided input to plant operation for functions that could trip or de-rate the unit within 15 minutes. A participant included megawatt sensing meters, for instance, after determining that misuse or loss of that device would affect reliable operation of the plant. Participants excluded analog devices or meters used for non-BES reliability functions.
HMI Workstation	Survey participants identified HMI Workstations as BES Cyber Assets where the HMI is a component of another system such as a PLC or DCS that were integral to the operation of the plant. Similarly, if the HMI is used in a system such as burner management, combustion controls, or turbine controls it was considered a BES Cyber Asset. In contrast, if the device is used in an application such as coal or ash handling and would not have a 15 minute impact to generation the system, participants did not identify the device as a BES Cyber Asset. In addition any HMI Workstation that was architected as read only nodes were not considered BES Cyber Assets.

Application Server	Survey participants indicated that they classified application servers at their generation plants as BES Cyber Assets where those application servers that were part of the DCS, supported systems such as acoustic monitoring and vibration control monitoring or could otherwise trip or de-rate the unit in 15 minutes. A participant explained their DCS engineering workstations are considered BES Cyber Assets because they have the capability to edit DCS logic and can affect any generating unit. Another participant noted that one of their generating facilities has vibration analysis connected to trip the unit so it would be considered BES Cyber Asset. Examples of application servers not classified as BESs Cyber assets were intelligent soot blowing, neural net, FIS, combustion optimization, and vibration analysis in other generating facilities.
Network Printer	None of the participants included network printers as BES Cyber Assets, for the same reasons as in other locations.
Data Server	Survey participants indicated data servers are BES Cyber Assets where they are used for plant functions that could trip or de-rate the unit in 15 minutes. Participants excluded data servers where the servers perform no reliability functions and do not meet the 15 minute adverse impact criteria.
Historian	A few survey participants indicated that they classified one or more historians at generation plants designated as are BES Cyber Assets where the historian was on a DCS cyber systems and the network for that particular process can be disturbed due to misuse and result in a trip or de-rate of a generating unit's output within 15 minutes. Other participants explained that their historians were used for historical trending and post-event information only and were excluded from the BES Cyber Asset definition.
Computer Networking	All of the survey participants identified computer networking devices as BES Cyber Assets as computer networking equipment is necessary for plant functions that could trip or de-rate the unit in 15 minutes.
Equipment Diagnostic / Maintenance	Survey participants identified some equipment diagnostic/maintenance devices at generation plants as BES Cyber Assets depending on the on where and what network the device is on (such as certain DCS cyber systems). Some participants excluded vibration control and acoustic monitoring devices from the BES Cyber Asset definition.
Fault Recorder	The survey participants indicated that fault recorders are not BES Cyber Assets because these devices are used for post event analysis.
IED / Relay	All of the survey participants identified some IED/relays as BES Cyber Assets. As one participant explained, the unavailability, degradation, or misuse of certain IEDs would prevent the protected equipment from performing its real-time function, resulting in an impact to generation within 15 minutes. Such devices were excluded, however, if they were used in an application, such as ash pumps or coal belts, which would not have a 15 minute impact to generation the system.
RTU	Most of the survey participants identified RTUs as BES Cyber Assets. One participant explained. However, that for RTUs that are located within generation PSPs, it did not designate them as BES Cyber Assets because they cannot affect generation within 15 minutes.
PMU	None of the survey participants indicated they have PMUs at generation plants.

PDC	None of the survey participants indicated they have PDCs at generation plants.
Precision Time Device	A survey participant identified precision time devices as BES Cyber Assets, explaining that a precision time device on certain of its DCS cyber systems would be considered a BES Cyber Asset depending on the impact to the generating unit(s) of the particular part of the process the historian is connected. If the network for that particular process can be disturbed due to misuse (denial of service) and result in a trip or de-rate of a generating unit's output within 15 minutes, the precision time device would be a BES Cyber Asset. The other participants did not indicate precision time devices since they are only used for post-event analysis and have no impact to the BES within 15 minutes.
Development & Testing	A survey participant identified development and testing devices as BES Cyber Assets, namely, the simulator for the DCS that does logic changes to see how the process responds. All other participants described development and testing systems as having no impact to the BES within 15 minutes.
Infrastructure Support	Survey participants indicated that infrastructure support devices are BES Cyber Assets if they are used in a system (i.e., DCS, burner management, combustion control, or turbine control) that could have a real-time impact. In contrast, if used in a system, such as coal or ash handling, that did not have a 15-minute impact, participants did not classify them as BES Cyber Assets.
Other	N/A

IV. *Other Locations*

The Implementation Survey participants indicated that, as of the time of the survey, they have not identified any Cyber Assets at BES Facilities outside of control centers, transmission stations/substation, and generation plants that are categorized as BES Cyber Assets.

Description of Cyber Asset Types

The following is a description of the Cyber Assets listed in the tables above.

1. <u>Control Center</u>

- **Application Server**: Traditional computer used for executing Bulk Electric System operations applications such as status monitoring, limit checking, alarm generation, log management, automatic generation control (AGC), economic dispatch, interchange scheduling, unit scheduling, state estimation, contingency analysis, power flow analysis, switching studies, etc.
- **Data Server:** Similar to an application server, but primarily used to provide data to application servers. Data servers include "traditional" servers running database software with locally attached storage, as well as network-attached storage servers (disk servers).
- **HMI (Human Machine Interface) Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human grid operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Data Acquisition Server**: Communications front-end processors used to communicate to other computer sites, control centers, field devices, or generation plants by receiving data from remote sites, process the data into local format, and store it for local use. Some data acquisition servers contain specialized hardware used to communicate to field devices; other data acquisition servers receive data via computer network connections.
- **Data Interchange**: Communications servers (e.g. ICCP servers) used to communicate inter-site data between control centers and other facilities that serve a BES function.
- **Phasor Data Concentrator (PDC)**: A device that manages data feeds from multiple Phasor Measurement Units (PMUs).
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, security event and incident management systems, EACMS, etc.
- **Communications Processing Devices**: Devices used to perform protocol conversions, encapsulate serial data into a routable protocol, encrypt communications, etc.
- **Diagnostic Devices**: Devices used to troubleshoot hardware or software; at a control center diagnostic devices are most often attached to the local area network but could be attached to other Cyber Assets. Diagnostic devices can be normal Cyber Assets such as laptop computers or specialized diagnostic equipment.

- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the Transmission elements for after-the-fact analysis.
- **Historian**: Generally, a combination of computer server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Situational Awareness**: Systems used to provide situational awareness in a real-time Bulk Electric System operations environment (e.g. video map-boards, tile map-board controllers, video trending).
- **Precision Time Device:** Device used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Training Simulator**: Computers (including application servers, database servers, HMI) that are used to train operators on various power system operations scenarios, and to test new operational procedures for validity.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, database updates, and power system model changes prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Marketing Systems**: Systems supporting marketing functions that may be located inside ESPs containing BES Cyber Systems. Examples include OASIS calculators, market pricing systems, market clearing systems, market billing systems, etc.

  Other: Any other Cyber Asset not described above. Please specify the application or function.

2. <u>Transmission Station / Substation</u>

- **Intelligent Electronic Device (IED) / Protective Relay**: IED or relay device protection system used to sense fault conditions (e.g., on Transmission lines), and take rapid autonomous actions to isolate the fault to prevent cascading fault conditions or equipment damage
- **Remote Terminal Unit (RTU)**: A device or system used to send telemetry data from the substation to the control center, and to receive control commands from the control center.
- **Programmable Logic Controller (PLC)**: Substation automation device used to coordinate actions taken by multiple IEDs, or when processing capabilities beyond the capability of an IED are required.

- **Data Concentrator**: A device or system used to collect data from multiple IEDs and provide a single data interface to the RTU.
- **Meter / Indicator**: A device used to provide local readout of values (e.g., bus voltage) or indication of status (e.g., breaker open/close). Meters / indicators may also collect and transmit values to other Cyber Assets.
- **Intelligent instrumentation**: Primary instrumentation used to sense values (e.g., voltage, current) or status (e.g., breaker or switch position). Primarily used by IEC 61850 enabled substations.
- **Tap Changer**: A device located on a transformer that allows the transformer winding ratio to be controlled remotely.
- **HMI Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, EACMS etc.
- **Communications Processing Devices**: Devices used to perform protocol conversions, encapsulate serial data into a routable protocol, encrypt communications, etc.
- **Equipment Diagnostic / Maintenance**: Devices used to monitor the behavior of the substation computers, calibrate the instrumentation, or diagnose problems with the control or networking components.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the Transmission elements for after-the-fact analysis.
- **Phasor Measurement Unit** (**PMU)**: A device that performs high-speed monitoring and analysis of voltage and current values and waveforms. In some cases, PMU data is used for after-the-fact analysis; in other cases, PMU data is used for real-time autonomous control.
- **Phasor Data Concentrator** (**PDC)**: A device that manages data feeds from multiple PMUs.
- **Historian**: Generally, a combination of computer server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Precision Time Device:** Device used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.

- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, and database updates prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Other**: Any other Cyber Asset not described above. Please specify the application or function.

3. <u>Generation Plants</u>

- **Controller (PLC)**: First level control system, used to coordinate the actions of a specific set of sensors and actuators. Controllers are programmed to take the input of specific sensors, process their data, and send output control commands to actuators, generally with a feedback loop to assess the impact of the control action, and take additional control actions if necessary. Individual controllers send status and values to higher level controllers and application servers for supervisory control and display to operators.
- **Distributed Control System (DCS)**: Modules, processors, communications relays, and other sub-components that control the plant and allow operators at HMI interfaces to manipulate the plant.
- **Sensor / Actuator / Transmitter**: Primary input and output elements in a distributed control system. Sensors sense process values (e.g., pressure, temperature); actuators invoke changes in the process (e.g., open and close valves, change the speed of motors), and transmitters provide the local interface between the sensor and actuator to the control system hardware. Modern sensors and actuators contain embedded transmitters, older sensors and actuators require transmitters to translate analog signals to digital signals, or to allow the analog control signals to travel longer distances.
- **Meter / Indicator**: Device used to provide local readout of values (e.g., pressure, temperature) or indication of status (e.g., valve position). Meters / indicators may also collect and transmit values to other Cyber Assets.
- **HMI Workstation**: A workstation computer consisting of display and keyboard attached to a small computer. HMI Workstations are used to provide human operators with status and values, and allow them to enter parameters to control the process.
- **Network Printer**: A printer that is attached directly to the network, and is therefore shared by multiple users and applications.
- **Application Server**: Traditional computer nodes used for executing Bulk Electric System operations applications such as plant optimization, or to coordinate the action of multiple independent control systems.

- **Data Server**: Similar to an application server, but primarily used to provide data to application servers. Data servers include "traditional" servers running database software with locally attached storage, as well as network-attached storage servers (disk servers).
- **Historian**: Generally, a combination of computer server and data server with specialized software used for storing a historical record of Bulk Electric System operations data. Historians also can be used to provide access to data outside of the control center without impacting the control center processing.
- **Computer Networking Devices**: Hardware used to provide connectivity between other computers. Examples include hubs, switches, routers, firewalls, intrusion detection/prevention systems, terminal servers, EACMS, etc.
- **Equipment Diagnostic / Maintenance Devices**: Devices used to monitor the behavior of the generation plant computers, calibrate the instrumentation, or diagnose problems with the control or networking components.
- **Fault Recorder**: Device used to detect faults and record the electrical behavior of the Transmission elements for after-the-fact analysis.
- **Intelligent Electronic Device (IED) / Protective Relay**: IED or relay device protection system used to sense fault conditions (e.g., on a generator bus), and take rapid autonomous actions to isolate the fault to prevent cascading fault conditions or equipment damage.
- **Remote Terminal Unit (RTU):** A device or system used to send telemetry data from the substation to the control center, and to receive control commands from the control center.
- **Phasor Measurement Unit (PMU)**: A device that performs high-speed monitoring and analysis of voltage and current values and waveforms. In some cases, PMU data is used for after-the-fact analysis; in other cases, PMU data is used for real-time autonomous control.
- **Phasor Data Concentrator (PDC):** A device that manages data feeds from multiple PMUs.
- **Precision Time Device:** Device used to synchronize the time on electronic equipment with a highly accurate reference such as a GPS master clock.
- **Development & Testing**: Computers (including application servers, database servers, HMI) that are used to develop and test new application programs, and database updates prior to their inclusion in the real-time operations environment.
- **Infrastructure Support**: Computers that provide support functions to other Cyber Assets, such as domain name system (DNS), active directory, certificate management, administrative workstations, patch management, etc.
- **Other**: Any other Cyber Asset not described above. Please specify the application or function.