Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans

Prepared by the Staffs of the
Federal Energy Regulatory Commission
and the
North American Electric Reliability
Corporation and its Regional Entities
January 2016

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

This report was prepared by the staff of the Federal Energy Regulatory Commission in consultation with staff from the North American Electric Reliability Corporation and its Regional Entities.

This report does not necessarily reflect the views of the Commissio

Table of Contents

I. Executive Summary

In September 2014, the Federal Energy Regulatory Commission (FERC or the Commission) initiated a joint staff review, in partnership with the North American Electric Reliability Corporation (NERC) and the Regional Entities,[1] to assess entities' plans for restoration and recovery of the bulk power system following a widespread outage or blackout.[2] The objective of the review was to assess and verify the electric utility industry's bulk power system recovery and restoration planning, and to test the efficacy of related Reliability Standards in maintaining and advancing reliability in that respect. The joint staff review was not a compliance or enforcement initiative. This report presents the results of that joint staff review.

In conducting this review, the joint staff review team gathered information from a representative sample of nine registered entities with significant bulk power grid responsibilities (the participants), including some entities that are registered with NERC in multiple functions.

The review team examined the restoration, response and recovery plans of each participant, along with supporting information. Documents reviewed included, but were not limited to, reliability coordinator-approved restoration plans, procedures for deploying blackstart resources, steady state and dynamic simulations testing the effectiveness of the plans, and cyber security incident response plans and recovery plans for critical cyber assets. The team also met with or conferred with the participants to discuss the above plans, as well as their experiences with recent restoration, response and recovery exercises or drills, and observed a number of restoration training exercises. The team assessed the relative strengths as well as any shortcomings of the plans across the various stages and topics of restoration, cyber security incident response and critical cyber asset recovery. The joint staff review team then reviewed the associated Reliability Standard requirements for clarity and efficacy to determine any reliability gaps, also taking into consideration relevant recommendations from the NERC-convened Independent Experts Review Panel (IERP).

---

[1] Pursuant to section 215(e)(4) of the Federal Power Act, NERC has delegated certain compliance and enforcement authority to eight Regional Entities.

[2] NERC maintains a Compliance Registry that identifies all entities, referred to as "registered entities," which must comply with mandatory Reliability Standards.

This report provides the team's observations on the participants' plans, assesses the related Reliability Standards, and makes recommendations for potential enhancements to the plans, related practices, and the provisions of certain Reliability Standards.[3]

Overall, the joint staff review team found that the participants have system restoration plans that, for the most part, are thorough and highly-detailed. The reviewed plans require identification and testing of blackstart resources, identification of primary and alternate cranking paths, and periodic training and drilling on the restoration process under a variety of outage scenarios.[4] Likewise, the joint staff review team found that participants had extensive cyber security incident response and recovery plans for critical cyber assets covering the majority of the response and recovery stages. In addition, the team observed that each participant has full time personnel dedicated to the roles and responsibilities defined in their respective response and recovery plans.

The joint staff review team identified several opportunities for improving system restoration and cyber incident response and recovery planning and readiness through, among other things, improvements to the clarity of certain Reliability Standard requirements. The joint staff review team accordingly recommends that measures be taken, including (in accordance with NERC's standards development process), considering changes to the current Reliability Standards to address the issues and recommendations as set out below and further discussed in the body of this report. In addition, the joint staff review team recommends that further studies be performed in certain areas, including those in which new Critical Infrastructure Protection (CIP) Reliability Standards have yet to go into effect.[5] Finally, the joint staff review team observed numerous beneficial practices employed by individual participants. The joint

---

[3] Appendix 4 includes a glossary of terms, and Appendix 5 includes a list of acronyms used in this report.

[4] A cranking path is a portion of the electric system that can be isolated, and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units. *See NERC Glossary of Terms*

[5] The joint staff review team recommends that FERC and NERC staff discuss, following report issuance, responsibility for performing, and prioritization of, the recommended studies along with the associated details to accomplish them.

staff team recommends that other registered entities responsible for system restoration, cyber security incident response, or recovery readiness consider incorporating similar practices into their plans and practices, where and as appropriate.

System Restoration Planning

Recommendations for Changes

1. **Clarify when system changes will trigger a requirement to update resto plans.** The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address the need for updating restoration plans for all system modifications that would change the implementation of an entity's restoration plan for an extended period of time, not just permanent or planned system modifications. In considering these measures, the kinds of events that may warrant an update to the system restoration plan should be identified, taking into account the length of time the system is affected, as well as the overall objective of ensuring that restoration plans are generally flexible enough so that system modifications can be addressed without continuous updates. **[Section IV.E]**

2. **Verification/testing of modified restoration plan.** The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address the need for re-verification of a system restoration plan when a system change precipitates the need to determine whether the plan's restoration processes and procedures, when implemented, will operate reliably, i.e., when needed to ensure that the restoration plan, when implemented, allows for restoration of the system within acceptable operating voltage and frequency limits.[6] In considering such measures, the types of system changes that could impact reliable implementation of the restoration plan should be taken into account (e.g., identification of a new blackstart generator location or on redefinition of a cranking path). **[Section IV.G]**

3. **Operator training: Exercises on transferring control back to the balanci authority.** The joint staff review team recommends that measures be taken

[6] The Reliability Standards currently require verification of an applicable entity's system restoration plan every five years. While the review participants currently test and verify the effectiveness of their restoration plans following significant changes that could impact the viability of their plans, they are not obligated to do so under the current Reliability Standards.

(including considering changes to the Reliability Standards) to address system restoration training and drilling for transitioning from transmission operator island control to balancing authority ACE/AGC [7] control. **[Section IV.H.]**

Recommended Studies and Coordination Efforts

4. **Planning for loss of SCADA and loss of other data sources.** Given the possibility that Supervisory Control and Data Acquisition (SCADA) computer systems, [8] Inter-Control Center Communications Protocol (ICCP), or Energy Management System (EMS) functionality may be compromised during a major disturbance (e.g., portions of SCADA may not be available after a significant blackout), the joint staff review team recommends that further study be conducted to (a) assess system restoration plan steps that may be difficult in the absence of SCADA, ICCP data, and/or EMS; and (b) identify viable resources, methods or practices that would enable timely system restoration to occur absent SCADA/EMS functionality, which could then be incorporated into entities' system restoration training. The study should also examine and identify best practices that may be shared across the industry. Pending such study, individual entities should initiate or update consideration of resources, methods and practices they can use in these circumstances. **[Section IV.C]**

5. **Gain further understanding of recent blackstart resource changes.** The joint staff review team recommends study of the availability of blackstart resources, including the identification of strategies for replacing blackstart resources going forward and factors to be considered for such replacement resources (e.g., locational diversity, dual fuel, etc.). **[Section IV.D]**

6. **Gain further understanding of the use of direct current (DC) facilities fo restoration.** The joint staff review team recommends that a study be conducted to determine the benefits of including existing or future voltage source converter DC lines in system restoration plans. **[Section IV.D]**

---

[7] Area Control Error (ACE) and Automatic Generation Control (AGC) are mechanisms to assess and adjust the instantaneous difference between a balancing authority's actual and scheduled interchange.

[8] A SCADA system operates with coded signals over communication channels to monitor and provide control of remote equipment (using typically one communication channel per remote station).

7. **Blackstart resource testing under anticipated blackstart conditions.** The joint staff review team recommends a study be performed to identify options for expanding restoration plan testing beyond the currently-required blackstart resource testing, to ensure the blackstart resource can energize equipment needed to restore the system as intended in the restoration plan. Any expanded testing requirements should take into consideration whether such testing is practical while maintaining system reliability, and whether such expanded testing requirements could affect the identification of blackstart resources in the future. **[Section IV.F]**

8. **Obtaining insight from entities that have experienced a widespread out** The team recommends that applicable entities that have not recently experienced a blackout or other events which impacted, or could have the potential to impact, the viability of their restoration plans reach out to those who have experienced such events, in an effort to continuously improve their restoration plans. Entities could benefit from the sharing of experiences across different regions of the country to gain insight into events that may not have ever occurred locally, including:

    - Severe flooding and storm impacts on facilities and equipment depended on for system restoration;
    - Effects of extreme temperatures, including severe cold weather impacts on facilities and equipment depended on for system restoration; and
    - Preparedness training for the above impacts. **[Section IV.I]**

Cyber Incident Response and Recovery Plans

Recommendations for Changes

9. **Response and recovery plan ownership.** The joint staff review team recommends that cyber security incident response plans and recovery plans for critical cyber assets specifically designate accountability at the cyber asset level (e.g., EMS servers, remote terminal unit (RTU) concentrators, network routers, etc.). The team recommends that measures be taken (including considering changes to the Reliability Standards) to address this. **[Section V.A]**

10. **Require details on types of cyber security events that should trigger a r and reporting.** The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address the need for cyber security incident response plans to include details around the types of events that should trigger a response, and what types should be reported. While the team recognizes that CIP version 5 will require responsible entities to have processes to

identify cyber security incidents, consideration should be given as to whether any additional clarification or improvements are needed once some experience is gained with CIP version 5. **[Section V.C]**

11. **Use of technical expertise and advanced tools.** The joint staff review team has concluded that cyber event monitoring and response would be greatly improved by expanding the use of cyber security technical expertise and advanced technical tools, and recommends that measures be taken (including considering changes to the Reliability Standards) to address the use of these tools to improve cyber event monitoring and response. In considering such changes, it may be appropriate to allow for some experience with CIP versions 5 and 6. In addition, the team recommends that such measures clarify that these advanced tools and resources should be employed in a manner that does not negate the benefits by making the cyber security event monitoring process more cumbersome or unnecessarily burdensome. **[Section V.C.]**

12. **Recovery plan inventory assumptions risk.** The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to eliminate, to the extent possible, "inventory assumptions" in cyber asset recovery plans that could significantly affect prompt recovery of critical cyber assets. For example, entities may assume that hardware from external sources or other third-party vendor support needed for recovery of critical cyber assets will be available, without necessarily having measures to ensure availability. Likewise, entities may not consider interdependent or common-mode failure scenarios, which can create the need to recover multiple critical cyber assets concurrently from the same vendors. **[Section V.E]**

Recommended Studies and Practices

13. **Independent review of cyber security response and recovery plans.** The joint staff review team recommends that recovery plans for critical cyber assets and cyber security incident response plans be reviewed by an independent authority or third party for the purpose of supporting thoroughness and technical reliability, using a trusted or qualified third party to ensure a proper security review. **[Section V.F]**

14. **Exercises of response and recovery plans using paper drills.** The joint staff review team observed that participation in full operational exercises and other more complex simulations provides greater insight into the viability of a given cyber response and recovery plan, and believes that participation in such exercises by the industry is valuable for developing robust recovery and response plans. The joint staff review team recommends that applicable entities participate in exercise scenarios and simulations structured to gain insight into the viability of cyber response and recovery

plans (i.e., beyond paper drills and tabletop exercises), including testing for interdependencies and other vulnerabilities. **[Section V.G]**

15. **Gain further understanding of response and recovery plan updating following testing or actual cyber events.** The joint staff review team recommends that a study be conducted to better understand the associated plan improvements made by entities where testing or an actual cyber event reveals the need or opportunity for improvements to a response and recovery plan. This study would support a better understanding of the effectiveness and existence of continuous improvement processes. In addition, the study should examine and identify best practices with regard to the types of plan improvements made from entities' analyses of actual cyber events and/or testing. Such information could reveal the need or opportunity for improvements to other entities' response and recovery plans and be a valuable component of a continuous improvement process. **[Section V.H]**

Observed Practices for Consideration

Throughout its review, the joint staff review team found that the participants have many practices and protocols that serve to enhance their restoration and recovery planning and readiness but go beyond the requirements of the Reliability Standards. The joint staff review team recognizes that these practices may not be appropriate for all entities in all situations, but believes that wider understanding and incorporation of these practices will have significant value to certain entities and to the industry as a whole. Examples of these beneficial practices include the following:

- Some review participants include in their restoration plans illustrations and accompanying steps to assist operators in system restoration. Illustrations and guidelines include electrical (i.e., one-line) diagrams, tables, or charts of reference information to augment the steps of restoration. The inclusion of these additional details can be a valuable aid to operators in the execution of the plan.

- Many participants have extra personnel in place to augment operators and other support staff during system restoration. The additional personnel can perform tasks in support of the restoration effort, including performing off-line power flow studies, so system operators are able to focus on essential system restoration tasks with minimal distractions.

- Some participants perform exercises or drills that involve the actual transfer of control center operations to an alternate site for a period of time, in order to test the functionality of the recovery resources. This practice goes beyond the requirements of the Reliability Standards to provide a more realistic test of

response and recovery readiness. The actual evacuation and verification of functionality of recovery resources can reveal unknown issues or problems through use of the alternate site's cyber assets.

Such sound practices, which were voluntarily implemented by review participants, serve to enhance the industry's preparation for a major event, and provide training to recover more quickly and efficiently when an event occurs. A discussion of beneficial practices observed by the joint staff review team can be found in the relevant sections of this report.

II. Introduction: What are System Restoration and Recovery Plans and Why Are They Important?

In the United States, electric customers depend on reliable and continuous service. Unexpected loss of power is inconvenient. Moreover, sustained and widespread outages may lead to more severe circumstances that are potentially catastrophic. Typically, power losses are confined to relatively small areas of the electric system, and the vast majority of outages experienced by customers are the result of the loss of distribution level facilities.[9] Despite the overall reliability of the transmission system as a whole, however, widespread outages do occur, as seen with the August 2003 blackout, the September 2011 outages in Arizona and Southern California, and the outages caused by Hurricane Sandy in 2012.

These major events can cause significant disruption of the bulk power system, and often require the use of blackstart resources[10] and coordinated, multi-entity efforts to restore the system. Because these events are significant, although uncommon, it is critical that all entities potentially involved in the system restoration process be prepared to respond to potential widespread outage scenarios. This report focuses on evaluating the readiness of the electric utility industry to restore the bulk power system following a widespread outage.

While utilities have historically developed their own formal plans and procedures to restore their systems after widespread outages, they were not subject to a mandatory requirement to do so prior to the August 2003 blackout. Following that outage, Congress passed the Energy Policy Act of 2005, which, among other things, required the

---

[9] Generation or transmission line outages often do not impact electric customers. During storms, for example, one or more transmission lines may trip offline due to lightning strikes or other causes. However, customer service may not be interrupted because the transmission systems are typically designed to isolate the affected circuits and prevent a shutdown.

[10] Blackstart resources are generating units that have the ability to be started without support from the rest of the bulk power system, or are designed to remain energized without connection to the remainder of the bulk power system, and can be used to re-start other generating units as part of the process of re-energizing the system.

Commission to certify an independent Electric Reliability Organization (ERO) tasked with developing and enforcing mandatory reliability standards. NERC was certified as the ERO in 2006, and works with industry to develop mandatory reliability standards, the first set of which were approved by the Commission in 2007. [11]

One approved Reliability Standard, EOP-005-2 (System Restoration from Blackstart Resources), requires transmission operators and reliability coordinators to develop and maintain adequate system restoration plans. Specifically, each transmission operator is required to have a system restoration plan to reestablish its electric system in a stable and orderly manner in the event of a partial or total shutdown of its system. These plans are required to include necessary processes and procedures to cover emergency conditions and the loss of vital telecommunications channels. The standard also requires generator operators with blackstart resources to establish procedures related to those units, and to coordinate and communicate with other entities regarding the status of those units.

Although most entities have system restoration plans that cover multiple situations, the scope of the restoration plan required by the Reliability Standards is as follows: [12]

> The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service . . . . [13]

The Reliability Standards require that the system restoration plan restore "the shut down area to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System." [14]

---

[11] Electric power entities that own or operate infrastructure or systems that comprise the bulk power system are generally required to register with NERC and comply with the mandatory Reliability Standards, including those pertaining to system restoration.

[12] Some entities also have restoration plans or procedures to address restoration of services at the distribution level, which plans and procedures do not fall within the Commission's jurisdiction and are not the subject of this report.

[13] NERC Reliability Standard EOP-005-2 (System Restoration from Blackstart Resources) at Requirement R1.

[14] *Id.*

In addition to the system restoration plan requirements, the approved Reliability Standards also require applicable entities to have a *cyber security incident response plan* as well as a *recovery plan for critical cyber assets*. In most cases, the computer systems used to remotely monitor and control the electric system are identified as "critical cyber assets," and therefore subject to the Reliability Standard requirements related to cyber security responses and critical cyber asset recovery plans. Having appropriate cyber security and cyber response plans in place is thus a critical part of system restoration.

III. Joint-Staff Review Process

The primary objective of the joint staff review was to assess participants' plans and readiness for system restoration and recovery efforts following a widespread outage, and to evaluate the efficacy and clarity of the associated Reliability Standards to help ensure the adequacy of these plans. The objectives of the review included:

- Gathering information via outreach to a representative sample of selected entities with significant bulk power system responsibilities.
- Gaining an understanding of the overall state of restoration plans by comparing and contrasting their content, scope and interrelationships.
- Assessing the clarity of the Reliability Standards in supporting the adequacy and efficacy of restoration and recovery plans.
- Identifying good industry practices and making recommendations to ensure that effective restoration and recovery plans are in place to support reliability. [15]

The recovery and restoration plan review focused on reviewing the adequacy of three Reliability Standards (as discussed further below in Section IV):

- EOP-005-2 System Restoration Plans from Blackstart Resources
- CIP-008-3 Cyber Security—Incident Reporting and Response Planning
- CIP-009-3 Cyber Security—Recovery Plans for Critical Cyber Assets [16]

---

[15] *See* Appendix 2 – Request Letter for Participation in Reliability Assessment at 2 (sent Sept., 2014).

[16] The cyber-related Reliability Standards reviewed reflect the CIP standards currently in effect, i.e., CIP Version 3. The Commission has approved a revised version of CIP

The joint staff review team adopted a collaborative model for conducting the review. Subject matter experts from the Commission, NERC and the Regional Entities collaborated to form the review team, collectively providing the necessary planning, operations and cyber security expertise.[17]

Once assembled, the joint staff review team identified a representative sample of entities with significant bulk power system responsibilities, to achieve comprehensive review of the wider area restoration capabilities.

The joint staff review team contacted each identified entity to request its participation. All contacted entities agreed to participate in the review, and without exception, were exemplary in their cooperation with the joint staff review team, sharing the detailed technical rationale behind their restoration and recovery plans. The joint staff team commends the participating entities for their open and active contributions.

In order to facilitate a full and open discussion of each participant's methodologies and strategies for restoration, their underlying rationale, and the resulting list of critical assets, the joint review team agreed not to disclose entity-specific information outside each review group. This report accordingly provides the results of the reviews without attribution to individual entities.

The joint staff review team reviewed each participant's restoration and recovery plans and supporting information, and engaged in discussions with the participants to gain additional information and insights regarding individual plans. The reviews were comprehensive and thorough, with some involving on-site visits. The team evaluated the participants' plans and procedures for each stage of restoration, response, and recovery, to ensure completeness and consistency of review from one participant to the next.

---

standards, i.e., CIP Version 5, which will become enforceable for certain assets starting on April 1, 2016. *See Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013). While the joint staff review team focused on the currently-effective CIP Version 3 Reliability Standards in conducting their review, this report also indicates whether the team expects CIP Version 5 to address or otherwise affect an identified area of concern.

[17] Appendix 1 lists the joint staff review team members.

For the various stages and topics of restoration, cyber security incident response and critical cyber asset recovery, the team undertook the following steps:

Step 1: Gain understanding of participants' bulk power system restoration and recovery reliability activities;

Step 2: Identify strengths and shortcomings of individual plans and procedures;

Step 3: Using the results from steps 1 and 2, perform an assessment of relevant Reliability Standards; and

Step 4: Form recommendations to improve reliability.

IV. Review of System Restoration Plans and Related Standards Assessment

The joint staff review team reviewed the system restoration plans, procedures and resources of the participants to assess their readiness to restore the electric system to a normal condition in the event of a partial or total system shutdown. This report provides a breakdown of the review by various restoration topics. These topics include:

- Strategies and Priorities for Restoration;
- Roles, Interrelationships and Coordination;
- Situational Awareness Tools for Quick and Orderly Restoration;
- System Restoration Resources;
- Island Development and Synchronization;
- Testing of System Restoration Resources;
- Testing, Verification, and Updating of System Restoration Plans;
- System Restoration Drills and Training Exercises; and
- Incorporation of Lessons Learned from Prior Outage Events.

As noted above, included at the close of each topic is analysis of the participants' plans against the relevant Reliability Standards, to see where improvements in clarity or

efficacy of the standards may be warranted. In reviewing the Reliability Standards, the team also considered relevant recommendations for improvement to Reliability Standards as made by the IERP. [18]

A. Strategies and Priorities for Restoration

1. Summary

The overall objective of a restoration plan is timely restoration of the transmission operator's system, with priority placed on restoring the interconnection as a whole. To accomplish this, the transmission operator assesses the initial conditions to determine the restoration strategy. In its review of the participants' strategies and priorities for restoration, the joint staff review team examined initial assessments to determine various restoration plan strategies, and priorities for restoring loads and tie-lines.

As described below, the joint staff review team found that the participants' restoration plans address the need to identify restoration strategies and priorities. The team found that the participants' plans require highly-detailed initial status assessments using templates, computer applications, or forms to identify and convey to system operators and reliability coordinators the extent of the outages and affected facilities. These initial status assessments ultimately determine the strategy(ies) to employ for restoration.

The joint staff review team concludes, as a result of its examination of the plans, that the relevant EOP-005-2 Reliability Standard requirements that address system restoration strategies and priorities are clear and effective. The joint staff review team also observed certain practices and approaches that appear to enhance an entity's ability to assess or address a given disturbance, and recommends that applicable entities consider implementing these approaches in their own restoration plans. Observations by the joint staff review team are detailed below.

2. Review of Participants' Restoration Plans

a) Initial Assessment of Conditions

All of the participants' restoration plans require an initial assessment of the status of the system as a critical first step, including assessment of the status of major transmission

[18] See NERC, *Standards Independent Experts Review Project: An Independent Review Industry Experts* (June 2013) http://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/Standards_Independent_Experts_Review_Project_Report.pdf) (IERP Report).

lines, generating units available to be ramped up or started on demand, and electrical islands that may still be operating. This initial assessment allows the participants to determine an appropriate restoration strategy(ies).[19]

All of the participants rely on SCADA as their primary data gathering tool during the assessment phase following a disturbance. Some of the participants have recognized the likelihood that their data reporting systems will be inundated with data during a large disturbance, and are using special algorithms to filter the data, to assist in evaluating events and alarms and other status indicators received. These participants indicated that they developed this approach in response to previous events, and the joint staff review team believes that these kinds of alarm management approaches can enhance an entity's ability to accurately assess system conditions and initiate prompt system restoration.

One reliability coordinator has instituted the use of a status reporting form as part of its restoration plan. All transmission operators within its footprint are familiar with the form, as it is used during the reliability coordinator's regular restoration training drills. The joint staff review team found that use of a status reporting form, including training and drilling based on that form, should improve the speed and accuracy of reporting and appears to be a best practice worthy of consideration by other reliability coordinators. Use of a common form also enables the integration of individual reports from multiple entities to better enable the reliability coordinator to understand the state of the system within its footprint.

b) Restoration Strategies

All of the participants' restoration plans are designed around a worst-case, total blackout scenario baseline, although several participants' plans include a range of scenarios in addition to a full blackout, as discussed further below.

Participants employ an "inside-out" island development strategy, in that the viability of their plans is not dependent on outside sources (i.e., not dependent on tie-line connections with other entities for restoration). The only exception is for pre-arranged external blackstart resources. Since most participants use more than one blackstart generator in their system restoration plans, their plans generally address the simultaneous

[19] In making their initial assessment, the participants analyze a range of factors, including, for example: (1) frequency monitoring locations for restoration; (2) availability and location of blackstart resources; (3) available transmission paths to start up generating plants; and (4) boundaries of energized areas and status of interconnected systems.

development of multiple islands, in which transmission and generation operators work together to develop electrical islands within their respective footprints. Developing multiple islands can limit the impact of an outage during restoration, by preventing problems experienced during restoration in one in-development island from affecting another island. In addition, it allows multiple areas to be restored at the same time.

The joint staff review team compared the island development methods contained in participants' restoration plans and procedures and found that several participants use a "core-island" approach, while others use a "backbone-island" approach or some combination of the two. The core-island approach involves the start-up of a blackstart generator, which is then used to energize a transmission cranking path and provide cranking power for a nearby generator and priority loads. Other loads are then added incrementally, and additional generators are synchronized via additional paths. With this incremental addition of generators and loads, the participant can develop a core electric island, while maintaining reserve generator capacity for island stability. The "backbone-island" approach involves starting up a larger blackstart generator and energizing higher nominal voltage and longer transmission lines (e.g. 230 kV, 345 kV) to develop a cross-system backbone to which core-developed islands can subsequently synchronize.

There are advantages to each island development approach. The core-island approach provides more island stability during the early stages of restoration. It also allows for underfrequency relay-controlled load to be restored sooner, but it may delay station service power to transmission substations, which may result in loss of SCADA for those substations due to back-up power supply (e.g., battery) depletion. The backbone-island approach can be a quicker method to restore auxiliary power to generators and transmission substations, including SCADA functionality. In addition, the larger amount of generation capacity brought online for the backbone method can provide transient stability and dynamic reactive reserve for voltage stability. However, this approach carries a risk of excessive voltages and may require additional voltage control facilities and equipment settings to mitigate these higher voltages.

As noted above, several participants include a range of initial scenarios in their restoration plans, (e.g., no blackout, with area internal to the transmission operator footprint becoming islanded) providing guidance to operators to respond to a wider range of emergency conditions. Also, based on their particular experience, lessons learned, and planning and engineering studies, some participants have identified areas vulnerable to a voltage collapse, and have developed strategies to contain the impact from such a collapse using automatic separation schemes. Thus, in addition to the total blackout scenario, some participants have incorporated these limited outage scenarios into their restoration plans to provide the operators a range of strategies and procedures for restoration.

c) Priority Loads and Tie-lines

All the participants include priorities for restoring loads in their system restoration plans, with the underlying objective of restoring the interconnection as a whole. Those transmission operators responsible for providing primary or back-up service to nuclear power plants prioritize the restoration of off-site power to those plants for safe shut-down. In addition, those participants serving metropolitan high-density loads place priority on restoration of those areas, recognizing the need to protect human safety.

Some participants' plans include criteria for identifying other high priority loads, including the following:

- Start-up power - otherwise referred to as "cranking power" - to non-blackstart generators that are designated to start-up quickly (e.g., in 4 hours or less) as part of the system restoration plan;
- Power to electric-powered pumps for natural gas pipelines that pressurize and provide the large volumes of natural gas deliveries to quick-start generators, such as combustion turbines;
- Auxiliary power needed for steam generator plants that do not have their own auxiliary power resources;
- Power to pumping stations for oil pipelines, nuclear military installations and floodwater or floodwall control installations; and
- Power to pumps that maintain oil pressure on underground electric transmission cables, to prevent failure of these cables during system restoration.[20]

All of the plans reviewed establish priorities for restoring load consistent with the requirements of the Reliability Standards (discussed further below), and most go beyond identifying the highest priorities and objectives to provide the system operator with a clear understanding of restoration priorities as restoration moves forward. For example, the joint staff review team observed that some participants' plans identify priority loads beyond those identified in the standards (i.e. nuclear power plants). These participants

[20] Distribution-level restoration plans also often identify higher-priority loads, including, for example, hospitals, critical water systems, and critical natural gas facilities.

indicated that identification of the next-level priority loads provides system operators with a clear understanding of the priority actions to take during system restoration.

All of the participants' restoration plans also recognize the priority of reconnecting to the rest of the system after a partial shutdown. However, the participants' restoration plans do not specify which external interconnection to restore first, i.e., they do not specify which interconnection neighboring transmission operators should restore first. The participants indicated that this practice was by design, in order to allow for flexibility in their restoration based upon the initial assessment of conditions. Participants emphasized that designing the plans to be flexible in this regard allows them to be adaptable to a range of initial conditions.

3. Related Standards Assessment

Reliability Standard EOP-005-2 has as its stated purpose to ensure plans, facilities, and personnel are prepared to enable system restoration from Blackstart Resources to assure reliability is maintained during restoration and priority is placed on restoring the Interconnection. The standard includes broadly written requirements for transmission operators to have strategies for system restoration based on expected blackout conditions, and procedures for restoring loads and interconnections, including prioritization and provision of off-site power supply for nuclear power plants. Sub-requirements R1.1 – R1.3 and R1.8 require transmission operators to have Reliability Coordinator-approved system restoration plans that include the following:

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

. . .

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

Requirements R1.1-R1.3 and R1.8 allow for flexibility in identifying strategies and priorities for restoration, which the team found to be appropriate, since strategies and

priorities for each entity would be different based on the entity's size, system topography, etc. Moreover, while certain standard requirements allow entities the flexibility to determine the level of detail to include in their restorations plans, this flexibility is balanced by the fact that Reliability Standard EOP-005-2 also requires simulation testing of the plan (R6) and reliability coordinator review and approval of each entity's plan (R3). This approach is supported by the joint staff review team's observations that, consistent with the requirements of Reliability Standard EOP-005-2 Requirements R1.1, R1.2, R1.3, and R1.8, the participants' plans each include detailed strategies and priorities for restoration under varying circumstances. Thus, the joint staff review team did not identify any issues related to such strategies and priorities that would suggest that modification of these requirements or other additions to the Reliability Standards is needed in this regard. The joint staff review team found that participants' plans include highly-detailed initial assessments, often involving the use of templates or forms to identify and convey the extent of the outages and affected facilities, to ultimately determine the strategy(ies) to employ for restoration. In addition, all participants' plans require restoration strategies to: be coordinated with the reliability coordinator's high-level strategy of restoring the interconnection (R1.1); clearly identify as a top priority re-establishing off-site power supply to nuclear power plants (R1.2), and identify priority loads for restoration (R1.8).

Finally, consistent with Requirement R1.3, all participants' restoration plans include procedures for restoring interconnections with other transmission operators under the direction of the reliability coordinator. While the plans did not place any priority on restoration of the connection with one transmission operator over another, the joint staff review team considers this to be appropriate given that restoration priority should depend on the initial assessment of conditions. The joint staff review team concurs with participants that prioritization of restoration of particular interconnected transmission operators should not be required.

4. Observed Practices for Consideration

In evaluating participants' strategies and priorities for system restoration, the joint staff review team observed the following practices and recommends consideration of them by entities:

- Some participants' plans include steps for addressing a range of scenarios in addition to a total blackout, including:
    - transmission operator area islanded
        - area within the transmission operator footprint becomes islanded, no blacked out area

- transmission operator area separation occurs from the rest of the interconnection, no blackout area

- transmission operator area blacked out with external/interconnection assistance available to aid in restoration

- transmission operator area blacked out without external/interconnection assistance available to aid in restoration

- transmission operator area becomes split (areas expected to break apart) in some pre-determined manner, requiring use of restoration plan processes to re-establish connection

Addressing multiple scenarios in the restoration plan provides flexibility and adaptable guidance for the operators to follow, enabling them to better respond to a wider range of emergency conditions.

- Some participants have highly-detailed load restoration priority guidance when developing their restoration plans, such as criteria for identification.

- Some participants employ applications, algorithms or other sorting and filtering mechanisms to analyze the high influx of alarms and other status-related data that may accompany a disturbance.

- Some participants use status reporting forms to expedite and clarify reporting of facility status information, and include the use of such forms in their restoration training and drills.

B. Roles, Interrelationships and Coordination

1. Summary

It is crucial that affected entities understand each other's roles and expected responsibilities in restoring the system to interconnected operations. The joint staff review team accordingly examined how the participants' restoration plans and procedures address or define the roles of the various entities involved in or affected by the participants' system restoration plans. The joint staff review team examined:

- Functional roles and interrelationships, according to NERC registration;

- Contractual roles and interrelationships, such as those covered by agreements or arrangements;

- Actual operational roles and interrelationships, such as those understood to exist based on participant discussions; and

- Coordination and communication that occurs during system restoration.

The joint review team found that participants' restoration plans address the respective roles of each entity involved in the restoration plan and are organized accordingly, with several that include tables of internal tasks or responsibilities, and of tasks expected of and approvals needed from the other entities involved in restoration. The joint staff review team determined that the participants' restoration plans, together with any related arrangements, are generally clear and sufficient in defining the roles and relationships among entities.

2. Review of Restoration Plans and Related Arrangements

Of the nine registered entities that participated in the review, the functional entity categories for the participants reviewed are as follows:

- Three entities were registered as reliability coordinators;
- Seven entities were registered as transmission operators;
- Five entities were registered as transmission owners (three of which were also registered as the transmission operator);
- One entity was registered as a generator operator;
- Two entities were registered as generator owners (one of which was also registered as the generator operator); and
- Five entities were registered as balancing authorities.

Two of the participants that perform transmission operator tasks have local control centers and operators who maintain SCADA-control of transmission facilities, but are not registered as transmission operators, and as such, are not required under the Reliability Standards to have a restoration plan that is approved by the reliability coordinator. However, the joint staff review team found that these two entities have detailed restoration procedures, which were prepared in coordination with, or as an appendix to, their respective transmission operator's restoration plan. The steps covered in these transmission owners' restoration procedures are similar to those covered in the transmission operator's system restoration plan, including, but not limited to: strategies for system restoration, steps for providing nuclear power plant off-site power, procedures for restoring interconnections with external entities and identification of cranking paths and initial switching requirements.

The review team also examined the following arrangements affecting restoration plans and the implementation of those restoration plans:

- Coordinated Functional Registrations: Some transmission operators have coordinated functional registrations with other transmission operators, covering responsibilities that include system restoration. A coordinated functional registration represents an agreement between two or more registered entities sharing and/or splitting compliance responsibility for requirements/sub-requirements within particular Reliability Standard(s).[21]

- Transmission operator-transmission owner member agreements or operating agreements: In some situations, a transmission owner may not also register as the transmission operator with NERC, although it does retain some operational control over transmission facilities. In this arrangement, the transmission owner's system operators (i.e., those that have control room operators with direct operational control of transmission facilities) are given authority to take actions to operate their system with transmission operator oversight, including actions required during system restoration.

- Blackstart generator agreements between transmission operators and generator operators: Entities have established blackstart service agreements that provide performance specifications for the blackstart unit. Some entities have blackstart resource agreements for resources located outside of the transmission operator footprint.

The joint staff review team determined that the participants' restoration plans, together with any related arrangements, are generally clear and sufficient in defining the roles and relationships among entities. For all of the arrangements reviewed, participants who had delegated restoration tasks through contractual arrangements or coordinated functional registrations included tables of tasks or responsibilities defining the roles, tasks and approvals needed by each entity involved in restoration. Such tables and charts provide clarity and reduce confusion as to who is responsible for performing each task, and help to define the associated communication, coordination and approval protocols during system restoration.

---

[21] *See* NERC Rules of Procedure § 508 – Provisions Relating to Coordinated Functional Registration (CFR) Entities, http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20151104.pdf.

3. Related Standards Assessment

Reliability Standard EOP-005-2, Requirement R1, includes several sub-requirements that address the need for transmission operators to coordinate with other entities and define roles through the development of procedures as part of a system restoration plan (sub-requirements R1.1 – R1.3 and R.1.9). These sub-requirements state that the restoration plan must include:

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

…

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

In addition, EOP-005-2 Requirement R13 addresses one aspect of the specification of roles and relationships among entities participating in the restoration process:

R13. Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements.

As noted above, the joint staff review team determined that the participants' restoration plans and related arrangements are generally clear and sufficient in defining the roles and relationships among entities. Though the relevant Requirements provide broad coordination-related topics to be addressed in restoration plans, the restoration plans and related arrangements reviewed by the team provide for appropriate coordination with the reliability coordinator's overall strategy for restoring the interconnection (as required under Requirement R1.1). Likewise, the team observed that the individual plans adequately cover the roles and responsibilities of blackstart resources (as required in R13), establish procedures with nuclear power plants for restoring offsite power (as required in R1.2), and include the necessary reliability coordinator approval steps for restoring interconnections with other transmission operators (as required in R1.3). The

joint staff review team determined that EOP-005-2, Requirements R1.1 – R1.3, and R13 are clear and effective in supporting restoration plans. Participants appeared to have a clear understanding of the obligations set forth in these provisions, and no issues of ambiguities were raised in discussions with participants or reflected in their restoration plans.

While Requirement R1.9 requires the transmission operator to have processes for transferring authority back to the balancing authority in accordance with the reliability coordinator's criteria, the joint staff review team found that some restoration plans contain limited information on the triggers, steps involved, or checks necessary for that transfer. However, the team believes that any additional need for clarification and better understanding of the processes for transferring authority back to the balancing authority should be addressed through operator training, as further discussed in section IV.H - System Restoration Drills and Training Exercises.

Reliability Standard EOP-005-2 applies primarily to transmission and generator operators and, as such, does not require transmission owners or generator owners to have an approved system restoration plan. However, the joint staff review team found that some generator owners and transmission owners have active roles and responsibilities in system restoration in maintaining stable operation during island development.[22] In some instances, the team found that the transmission owner has a restoration plan in coordination with, or as an appendix to, their transmission operator's restoration plan (as described above). In each case reviewed where the transmission owner has control center operators with SCADA control of the facilities, the transmission owner has such a plan in place. The team did not assess generator operator blackstart procedures, as the scope of the project was focused on the restoration plans of the transmission operators and the procedures for using blackstart resources. The team noted that each involved or affected entity (including transmission owners and generator operators) appeared to understand its respective roles and relationships for system restoration. Accordingly, while further study of the dependency of transmission operators on transmission owners and generator

[22] The IERP recommended that generator owners, distribution providers, transmission owners, and generator operators should be required to have an approved system restoration plan in place (in addition to transmission operators as required in EOP-005-2, and reliability coordinators as required in EOP-006-2). See NERC, *NERC Standards Announcement: Posted - Independent Experts Scoring for Requirements Spreadshe* (hyperlink: "Independent Experts Scoring for Requirements Spreadsheet," http://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/Ind_Exp_Scoring_Req_Spreadsheet_Announc_082913.pdf) (IERP Scoring Sheet).

owners in the system restoration process may be warranted, the team did not identify any concerns as to the participants' understanding and acceptance of their role in system restoration and does not recommend modification of the Reliability Standards to address this issue at this time. However, there may be similarly situated entities that were not part of this review that warrant future examination of transmission owner and generator owner roles and responsibilities during system restoration.

4. Observed Practices for Consideration

In evaluating participants' roles and responsibilities for system restoration, the joint staff review team observed that most participants include tables of tasks or responsibilities defining the roles, tasks and approvals needed by each entity involved in restoration. Such tables and charts provide clarity and reduce confusion as to who is responsible for performing each task, and help to define the associated communication, coordination and approval protocols during system restoration. The joint staff review team recommends that other registered entities with responsibility for system restoration consider this practice if they do not already maintain tables or similar methods to clearly defines roles, tasks and approvals needed for restoration.

C. Situational Awareness Tools for Quick and Orderly Restoration

1. Summary

Through discussions with participants and review of their restoration plans and other pertinent procedures, the joint staff review team examined and compared the situational awareness tools used to plan and carry out system restoration. The team found that the participants' plans recognize the importance of maintaining access to vital system data during a disturbance, employing redundant, diversely routed communications systems and redundant EMS or SCADA systems. In addition, participants' procedures include strategies for addressing the loss of SCADA, EMS[23] or ICCP[24], calling for the dispatch of personnel to substations in the event of the loss of such systems. Situational awareness tools and their usage are addressed in Reliability Standards other than EOP-005-2. Given

[23] Energy Management System (EMS) is a system of computer-aided tools used by bulk-power system operators to monitor, control and optimize system performance.

[24] The Inter-Control Center Protocol (ICCP) allows the exchange of real time and historical power system information between entities, including status and control data, measured values, scheduling data, energy accounting data and operator messages.

the possibility that SCADA, ICCP or EMS functionality may be compromised during a major disturbance, the team recommends that a study be conducted to assess system restoration plan steps that may be difficult in the absence of SCADA, ICCP data and/or EMS, and to identify viable resources, methods or practices that allow timely system restoration to occur absent SCADA/EMS functionality, which could then be incorporated into entities' system restoration training.

2. Review of Restoration Plans and Procedures

All of the participants' restoration plans rely on the extensive use of SCADA systems in assessing system status and in carrying out the restoration process. The joint staff review team found that SCADA systems facilitate a number of restoration processes, including the operator monitoring of frequency and voltages to ensure stability of developing islands. Likewise, the team observed that SCADA facilities can be particularly useful in the synchronization and interconnection of separate islands. SCADA systems can be used to provide much of the system information needed to identify interconnection opportunities and to evaluate whether conditions necessary to initiate synchronization have been met, and can be used along with other tools to allow system operators to interconnect systems without substation operators on site. In addition to SCADA, participants' restoration plans rely on ICCP data and EMS to remotely monitor and control the electric system. Participants noted the difficulty involved in restoring the system in the event SCADA/EMS or ICCP data are not available. One participant commented to the team that, in the absence of SCADA, restoration would be a long, tedious process. Some participants have a primary and back-up EMS at multiple control center locations with the ability to fully use the EMS from each location. These levels of redundancy help to ensure that EMS and SCADA have high levels of availability for reliable operation of the bulk power system, including reliable restoration.

Despite the redundancy in EMS and SCADA systems, all participants plan for the possibility that SCADA and EMS may be partially or totally unavailable at some time during a restoration event. For example, portions of SCADA functionality may not be available after a longer-duration blackout due to back-up power supply (e.g., battery) depletion for unrestored substations. Participants have procedures for loss of EMS and SCADA that broadly apply during normal and emergency grid conditions, including during restoration events. In the event of an EMS or SCADA failure, participant system operators notify EMS, Information Technology (IT), and/or telecommunications staff responsible for resolving SCADA and EMS concerns. In addition, participants' plans call for system operators to dispatch field personnel to transmission stations, so that field personnel are ready to manually perform feasible restoration activities, and provide field equipment status and data, at the direction of the system operator. Furthermore, most participants plan for system operators to work with operations and/or planning engineers using off-line power-flow models to perform system studies if SCADA, EMS and associated power flow applications are not available. Some participants' operators use

off-line data tracking applications specifically developed for system restoration monitoring in the case of EMS unavailability.

The joint staff review team found that EMS/SCADA systems play a significant role in operators' decision-making during system restoration, and the unavailability of these systems following a major system disturbance can delay system restoration. Participants indicated that a priority is placed on recovering SCADA, because there is not currently an alternate means of restoring the system as quickly without SCADA. Dispatching personnel to substations is an option, but lacking alternative or supplemental tools and resources to provide timely situational awareness for operators' decision-making could delay or complicate restoration compared to using SCADA or an equivalent approach. While the restoration of SCADA functionality is thus important for restoration efforts, SCADA functionality is equally important for adequate situational awareness during any system condition (normal or emergency). Accordingly, SCADA system protection and recovery has implications beyond system restoration, which the team believes should be addressed in that broader context.

3. Related Standards Assessment

The Reliability Standard requirements that relate to communications and use of situational awareness tools are covered by Reliability Standards other than EOP-005-2, including communications standards (COM-001-1.1), and a number of current and under-development operational standards (TOP and IRO). This report makes no recommendations as to those Reliability Standards.

4. Recommendations

Planning for loss of SCADA and loss of other data sources. Given the possibility that SCADA, ICCP or EMS functionality may be compromised during a major disturbance (e.g., portions of SCADA may not be available after a longer-term blackout), the joint staff review team recommends that a study be conducted to (a) assess system restoration plan steps that may be difficult in the absence of SCADA, ICCP data, and/or EMS; and (b) identify viable resources, methods or practices that would enable timely system restoration to occur absent SCADA/EMS functionality, which could then be incorporated into entities' system restoration training. [25] The study should also examine and identify best practices that may be shared across the industry. Pending such study, individual

[25] The joint staff review team recognizes that the study may be accomplished by performing analyses regionally, where there may exist different capabilities from one area to another.

entities should initiate or update consideration of resources, methods and practices they can use in these circumstances.

5. Observed Practices for Consideration

In evaluating each participants' approach to the use of SCADA, EMS and other situational awareness tools during system restoration (through site visits and discussions), the joint staff review team observed the following practices and recommends that other entities consider adoption of these practices :

- Remote monitoring of parameters necessary to synchronize islands and performance of remote synchronizing of islands.

- Provision of tools for system operators and support staff to allow them to efficiently process the numerous alarms received during the assessment phase of restoration. Participants who used such tools indicated that processing the alarm data quickly offers insight into the initial cause of the event, as well as provides information on the status of equipment after the event and during restoration.

- Use of cranking path displays, highlighting the cranking path transmission substations and transmission lines between the blackstart generator-substation and the next unit to be started.

- Use of SCADA displays which provide underfrequency load shedding (UFLS) load-relay substation locations with UFLS-controlled load values totaled, helping to improve island stability management where UFLS is integral to participants' restoration plans.

D. System Restoration Resources

1. Summary

The joint staff review team examined how the participants' restoration plans and procedures addressed the various resources needed for system restoration, focusing on blackstart generators (including their characteristics and procurement), communications, control center and field resources, and direct current transmission resources.

The joint staff review team found that the participants' restoration plans and procedures address the necessary identification and dedication of blackstart and other resources for system restoration, and the team did not identify any clarity or efficacy concerns with the Reliability Standards based on this area. Specifically, the team found that participants' restoration plans identify system restoration resources and their characteristics, including, at a minimum, blackstart resources' name, location, type, and MW and MVAr capacity, and identify personnel and their assigned responsibilities during system restoration.

Many participants indicated, however, concern about the future availability of blackstart resources currently relied on for system restoration. The joint staff review team recommends further study to gain a better understanding of this issue and to identify strategies for identifying other blackstart resources. Additionally, industry experts from the joint staff review team provided information on recent advances in voltage source converter technology that could facilitate system restoration efforts. The team recommends that the benefits of including voltage source converter DC lines in system restoration also be further studied.

2. Review of Restoration Plans

a) Blackstart Generators - Characteristics and Procurement

Blackstart units are selected, sited and adapted to their service areas, and participants' plans accordingly include a wide of range of blackstart resources. The participants' plans take different approaches to the use of power from blackstart resources, with some participants using power from blackstart units to energize priority loads (before providing auxiliary power to other generators), and others using power from blackstart resources to supply auxiliary power to larger units first during system restoration. The blackstart generators included in the participants' plans range in size from small (e.g., 25 MVA) to larger units (e.g. 100-200 MVA), or even banks of units, exceeding 1,000 MVA in capacity. Some participants rely on a single unit while others included multiple units in designated islands.

Participants needing to procure blackstart services generally have strategies and procedures in place for procurement. Based on the review of participants' plans, the joint staff review team observed that the period for procuring blackstart resources ranges from two to five years. The observed strategies and approaches to such procurement include the following:

- Some participants make an initial determination whether an existing facility can be retrofitted to make it blackstart capable, or whether a new facility can be contracted for blackstart service.

- Some participants may agree to provide a contribution towards a feasibility study that will cover the installation, technical capabilities and cost of installing blackstart capability at the site.

- Some participants may deal with multiple providers simultaneously to determine the most economic and efficient option. In general, the process involves a request for proposals from generator operators to provide blackstart service followed by a determination of the most efficient arrangement/allocation of blackstart resources.

- Where the removal or retirement of existing blackstart units from service creates the need for a blackstart resource, some participants issue requests for proposals to replace the retired units.

- One participant instituted a commitment period for blackstart generators of three years and required that a blackstart generator operator provide a two-year notice to cease providing blackstart service. This requirement allows for timely procurement of replacement blackstart resources in the affected zones.

Participants consider various parameters when selecting or procuring a blackstart resource, including geographic area, the capacity and reactive capability of blackstart generators, start-up time,[26] and proximity to priority load and results from computer simulations of cranking paths to determine viable blackstart solutions. In addition, some participants require the provider of new blackstart services to verify that it is capable of providing the contracted service, through an assessment at commissioning.

Participants also consider the proximity of generator fuel supplies and electric transmission facilities. Some participant transmission operators specifically identify areas within their footprint where it would be beneficial to locate blackstart resources. These transmission operators identify cranking paths for supplying blackstart generation from multiple areas to meet priority load requirements, such as supplying offsite power to a nuclear power plant. Some participants also allow blackstart units to be physically located outside their footprint, as long as the blackstart resource and cranking path(s) to receive the blackstart power are appropriately identified. The advantages of these analyses and arrangements can include improved restoration speed and efficiency, meeting priority load restoration timing requirements and eliminating a blackstart resource shortage in an area.

Finally, some participants take into account the value of diversifying the location of their blackstart resources, to mitigate the risk of multiple blackstart units being unavailable due to a single-point loss or failure. The joint staff review team believes that this is a practice that should be considered by other industry participants in appropriate circumstances.

Regarding the amount of blackstart resources, participants identify blackstart units to meet priority load requirements in alignment with their restoration strategies, and most of

[26] The start-up time for blackstart units in the reviewed plans ranges from five minutes to several hours. Although not a requirement, a shorter start-up time is desirable to aid in the speedy restoration of the system.

the participants reviewed have multiple blackstart resources.[27] Some participant transmission operators require that the capability of the identified blackstart units be large enough to provide sufficient power (MW) to restore priority loads and have sufficient reactive capability (MVAr) for voltage control. Others require that the total generating capacity of blackstart units be a certain factor above priority loads.[28]

Participants' blackstart resources include a mix of coal and gas-fired steam units, gas combustion turbines, and hydroelectric units. In order to ensure consistent access to fuel, the participants have taken the following measures:

- To ensure that gas supply to blackstart generators is not interrupted during restoration, some participants include gas compressors as priority loads.

- Most participants' restoration plans have blackstart units with dual fuel capabilities (using both oil and gas). One participant reported that about fifty percent of its blackstart generation capacity has dual fuel capability. With the possibility of limited natural gas supply that may occur during a blackout, some participants with dual-fuel blackstart capability have procured onsite oil or gas, which could run the generator for a limited period (e.g., 48 to 72 hours).

- While some participants indicated that their hydroelectric blackstart generator output may be restricted during certain times of the year when water is low,[29] some participants' plans contemplate coordinating with environmental or other associated regulatory agencies in emergencies, e.g., through the issuance of waivers of environmental restrictions for brief periods of time.

---

[27] Some transmission operators plan for a minimum of two blackstart units for defined areas within their footprint to meet priority load and cranking path needs.

[28] For instance, one participant requires that the total capacity of blackstart units be maintained at 110 percent of the total priority load.

[29] Some participants indicated that at certain times during the year, their small hydro facility or pumped storage facility output may be restricted due to the amount of water stored or available in its reservoir. One participant with a pumped storage unit reported that a minimum amount of stored water is required in the reservoir to maintain the ability to blackstart. Other participants relying on hydroelectric blackstart services indicated that the environmental restrictions on their units are relatively minimal, and may only occur during periods when water levels at the hydro station are below what is necessary to sustain fish life or during periods of drought.

In addition to traditional blackstart units, which are able to start without power from the interconnection, some participants include generating units capable of automatic load rejection (ALR) in their restoration plans. These units are typically base load, coal fired units that have the ability to immediately disconnect from the grid during a blackout, but can continue operating as an island and can be used to re-energize the transmission grid during restoration by providing startup power to larger units, to load, and eventually to interconnect with neighboring systems. ALR units can be vital to these participants' restoration processes, as they can reduce system restoration time.

The joint staff review team observed that some participants have elected to start retiring some of these ALR units. In general, participants indicated that the availability of some traditional blackstart resources is being affected by recent changes in environmental emissions regulations and CIP Reliability Standards, and that some of these units are now being withdrawn as blackstart resources.

b) Direct Current Transmission Lines

The joint staff review team explored the role of direct current (DC) transmission lines during system restoration and recovery, and observed that DC transmission lines are not considered in the participants' restoration plans or restoration plan simulations. Most of the existing DC lines use "line commutated" converter technology, and this technology is not typically operable during the early stages of island development and restoration. In the participants' current plans and procedures, restoration of DC transmission lines occurs during the later stages of restoration. Some evidence indicates that it is more advantageous to use DC lines with voltage source converter technology during early stages of island restoration instead of reenergizing a long EHV, AC transmission line, since the latter creates high voltage issues that must be mitigated.[30] The joint staff review team accordingly sees value in studying the potential benefits of using DC lines with voltage source converter technology during early stages of system restoration.

---

[30] Voltage source converter technology uses transistors, specifically insulated gate bipolar transistors, which are semiconductor devices that act as switches in the converter but function differently from thyristors. Commutation during the inversion process (DC to AC conversion at the receiving terminal) will take place under all system conditions at the receiving end. This allows a voltage source converter to be used when the system is very weak or blacked out. In addition, a voltage source converter has the capability to control active and reactive power at the receiving terminal. For further information, see M. Davies, M. Dommaschk, J. Dorn, J. Lang, D. Retzmann, D. Soerangr, *HVDC PLUS – Basics and Principle of Operation* (2011).

c) Communications, Control Center, and Field Resources

The joint staff review team also examined the participants' deployment and use of communications, control center, and field resources (including personnel) in their restoration plans.

Communications Resources. Participants indicated that system operators primarily use dedicated telephone or radio for voice communications, which systems are typically redundant and diversely routed. Participants indicated that additional phone lines, cell phone, satellite phone, and Government Emergency Telephone Service cards are the primary back-up voice communications facilities. Participants also indicated that their back-up facilities are tested on a regular basis to ensure their operability. In addition, some participants have their control center staff perform normal operations occasionally using their various back-up voice communications facilities to ensure that system operators are familiar with the back-up facilities.

Control Center and Field Resources. The review showed that system restoration is controlled and directed by NERC-certified system operators (reliability coordinators, transmission operators, and balancing authorities). The participants' control centers are staffed with system operators 24 hours a day, seven days a week. These control centers plan for the use of additional system operator staff during a restoration event. Participants indicated that their system operators are assigned specific roles during a restoration event and are trained accordingly. In addition, participants indicated that they typically use additional personnel, planning engineers, operations engineers, schedulers, and others to aid and support the system operators during major storms or a restoration event.[31] Furthermore, participants' plans call for dispatch of field personnel to key transmission substations to perform activities at the direction of the system operator.

As discussed further below in the Testing, Verification, and Updating of System Restoration Plans section, the joint staff review team found that station batteries can be vital resources during system restoration, since they provide power to station equipment when system power is lost. Participants indicated that their station batteries are typically

[31] Participants indicated that one challenge faced during a restoration event is staff transportation. Since streetlights and public communications infrastructure may be affected, participants have found that their staff may encounter difficulty moving from one location to another. Therefore, their plans include notifying staff of assigned work locations so they know where to report given a restoration event. Also, the participants noted that system operators on shift when a disturbance occurs may have to work extended hours before additional staff arrives.

sized to provide adequate power for eight hours, based on estimated system restoration times. Some participants go beyond this typical approach, as follows:

- Some participants size batteries to provide power for a longer time (e.g. twenty-four hours) for certain substations that are a priority for restoration, for more remote stations, or where the participant anticipates difficulty reaching the station due to damage from a natural disaster (e.g., areas more prone to hurricane weather).

- Some participants use portable batteries and portable generators to supply station power if needed during restoration.

- Some participants install local generation at control centers and other key facilities as back-up power sources and test these generators regularly to ensure operability.

3. Related Standards Assessment

Under Reliability Standard EOP-005-2, Requirement R1.4, all transmission operators are required to identify each blackstart resource and its characteristics as part of the restoration plan. This sub-requirement provides that the restoration plan must include:

> **R1.4.** Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

Other system restoration resources, including communications, control center, and field resources, are covered by other Reliability Standards.[32]

The joint staff review team found that the participants' plans include identification of blackstart resources and characteristics, including name of each blackstart unit, MW, MVAr, location, size and fuel type. The team did not identify any clarity or efficacy concerns with Requirement R1.4. However, recognizing that changes may be occurring with the need to procure and identify different blackstart resources going forward, the

[32] For example, telecommunications resources are covered in Reliability Standard COM-001-1.1 Requirement R1, which currently requires that transmission operators provide adequate and reliable telecommunications facilities which are redundant and diversely routed. Reliability Standard EOP-008-1 requires that transmission operators include in their contingency plans monitoring and control of critical transmission facilities and substation devices during emergencies.

joint staff review team recommends further study regarding these changes as discussed below.

4. Recommendations

Gain further understanding of recent blackstart resource changes. The joint staff review team recommends study of the availability of blackstart resources, including the identification of strategies for replacing blackstart resources going forward and factors to be considered for such replacement resources (e.g., location diversity, dual fuel, etc.). A future study may include discussions with a representative sample of generation owners and operators to gain further understanding.

Gain further understanding on the use of DC facilities for restoration The joint staff review team recommends that a study be conducted to determine the benefits of including existing or future voltage source converter DC lines in system restoration plans.

5. Observed Practices for Consideration

In evaluating the participants' identification and use of resources necessary for system restoration, the joint staff review team observed the following practices and recommends consideration of them by other entities as appropriate:

- Some participants include generating units with load rejection capability in their system restoration plans, to speed up restoration and recovery.

- Some participants coordinate the use of blackstart facilities across multiple transmission service footprints, which can allow a blackstart generator to contribute in supplying an adjacent area's priority load.

- Many participants maximize the use of dual fuel blackstart units, in order to minimize the risk that the blackstart unit will not be available if one fuel is in short supply or otherwise unavailable at the blackstart unit site.

- Many participants have special procedures in place to augment operators and other support staff during system restoration. The extra personnel can perform tasks in support of the restoration effort, including performing off-line power flow studies, among other things, so system operators are able to focus on essential system restoration tasks with minimal distractions.

E. Island Development and Synchronization

1. Summary

The joint staff review team examined the review participants' approach to island development and synchronization. In doing so, the review team examined three key areas:

- Participants' cranking or restoration paths and methods to connect blackstart units to priority loads in preparation for the next units to be started;
- How frequency and voltage is managed during restoration; and
- How synchronization is performed with other islands and systems.

The review team found that island development protocols in the participants' restoration plans thoroughly cover the above areas. The joint staff review team concludes that the related Reliability Standard requirements are clear and effective for most aspects of island development and synchronization. However, as discussed below, the team recommends that measures be taken (including considering changes to the relevant Reliability Standards) to address the need to update restoration plans for any system modification that would change implementation of an entity's restoration plan for an extended period of time.

2. Review of Restoration Plans

a) Restoration Paths and Initial Loads Energized

Restoration Paths. The joint staff review team found that all of the participants' restoration plans include the identification of initial restoration paths originating from blackstart generator(s) to the initial loads to be energized.[33] The team found that the participants also take into account the possibility that transmission facilities may not be available as planned for system restoration, and have adopted one or more approaches to addressing that issue.

First, as noted earlier in the report, some participants that are more prone to severe coastal weather patterns have developed significant storm response plans in conjunction

[33] Initial loads include the entities' priority loads as described earlier, including provision of nuclear power plant off-site power, and generating plant auxiliary loads for the next unit(s) to be started.

with their system restoration plans. Storm response plans reviewed by the team typically include targeted repair and restoration efforts for lines comprising a restoration path. [34] Also, many participants include alternate or back-up cranking paths and priority load paths as part of their restoration plan, to be used in the event a primary path is unavailable. Participants indicated that providing path redundancy, alternate paths, or back-up paths in plans for system restoration is of critical importance in situations where loss of the primary restoration path is likely. Participants take different approaches in identifying these alternate paths, however. Most participants explicitly identify the alternate cranking path, or path from their blackstart generator to the priority load(s), including verifying the viability of the alternate path through simulation. Other participants test multiple paths for restoration, but allow the operators discretion to select the path during restoration based on the conditions at the time.

Participants that execute the SCADA steps to energize cranking paths typically include highly-detailed steps for energizing those paths in their restoration plans, along with subsequent restoration steps. These steps specify the breaker-by-breaker steps to energize the entire cranking or restoration path. Those transmission operator participants that have arrangements with transmission owners to execute the actual steps to energize cranking paths have restoration plans that are more principles-based. These plans include an explanation of the electrical characteristics and associated protocols (e.g., voltage monitoring and control during restoration switching steps) to be observed during restoration. In this case, the transmission operator/transmission owner plans are designed to complement each other, with the combination providing a highly-comprehensive restoration plan.

Initial Loads. The joint staff review team found that in managing island stability, the magnitude of the initial loads planned for energization varies based on the capacity of that participant's blackstart generation. As initial loads are energized, participants take into account that cold load pickup and load inrush currents will be multiple times greater than steady-state values when loads are first energized following a sustained blackout condition. Also, for the initial steps of island path development, participants typically avoid energizing UFLS-enabled load, since initial load pickups are expected to cause large deviations in frequency. If the frequency falls below underfrequency relay trip levels, the resulting load shed could result in high frequency on the developing system, and cause generators to automatically come off-line due to over-speed conditions. Some

[34] This includes the transportation and mobilization of personnel and use of equipment inventories of transmission line towers and transmission substation elements (e.g. power transformers, breakers, switches) to storm damage locations.

participants avoid energizing UFLS-enabled load in their restoration plan entirely. For those participants that include energizing UFLS load at some point in their restoration plans, the order of restoration is set such that UFLS load with the lowest underfrequency trip settings is restored first.

Most of the participants' restoration plans include guidelines or factors as to the increment of load to be energized, depending on system conditions, in order to maintain sufficient generator reserves to ensure stability. Examples of factors incorporated in various participants' restoration plans include:

- Maximum increment of load pick-up:
    - 5 percent of online generator capacity
    - 5 percent (steam units), 15 percent (hydro units), 25 percent (combustion turbine units), of online generator capacity
    - Lesser of 5 percent or 25 MW of online generator capacity
    - Lesser of 5 percent or 100 MW of online generator capacity
    - 100 percent of total energized UFLS load (for later stages of island development)
- Island generator reserves, to account for cold load pickup:
    - 50 percent of online generator capacity
    - Approximately eight times the increment of large blocks of load added

In addition to managing reserves for cold load pickup, after the initial stage of island development, participants also verify that enough contingency generation reserves exist to withstand the forced outage of the largest online generator.

b) Managing Island Frequency, Voltage and Stability

Frequency. Participants' restoration plans require certain generators to monitor and control the frequency of the island. For example, for islands under isochronous control, [35]

[35] An isochronous (or zero droop) generator governor maintains the same speed regardless of the load, and ensures that the frequency of the electricity generated is

the frequency control and metering is located at the isochronous generator. Also, for frequency monitoring by transmission operators, frequency metering data from multiple transmission substations is displayed via the EMS/SCADA system along with the generator frequency metering data. The joint staff review team found that monitoring system frequency at diverse locations across their footprint via SCADA can aid transmission operators not only in island monitoring and management of load pick-up, but also in detection of an islanded condition.[36] The joint staff review team found the specific frequency limits in the participants' restoration plans typically provide for larger deviations in frequency than are permitted under normal operations.

Participants' restoration plans vary in the level of detail regarding operator coordination between the transmission control center, blackstart generator(s), and other generator control rooms with respect to managing generator operation. Even those plans that are highly detailed as to SCADA switching steps (i.e., plans of participants that execute the actual SCADA steps), appear to lack guidance on how the system operators should work with the generator control room operators to coordinate the output and operation of multiple generators within the developing island. In many cases, based on the interrelationships of the entities sampled, the system operator tasked with coordinating generator control room operators is the transmission operator or local control center (transmission owner) operator, who only performs these tasks during restoration following a blackout or in a restoration drill.[37] Alternatively, a few participants have the generator control room operators manage a considerable amount of coordination of load pick-up, generator loading, and management of reserves.

Voltage. The joint staff review team found that the participants' plans reflect the critical nature of maintaining a stable voltage on the transmission system during restoration in

---

constant or flat. Isochronous control mode is used to control frequency in an island during system restoration.

[36] In some instances, entities monitor system frequency at diverse locations in their footprint via phasor measurement units (PMUs). During Hurricane Gustav in 2008, operators first detected the electrical island that resulted from the large-scale outage when operator-monitored PMUs showed diverging system frequencies.

[37] One participant explained that the role of managing frequency and stability by a transmission owner/transmission operator is infrequent, and that these operators take on a "pseudo" balancing authority role during restoration.

order to successfully reenergize the grid. The review team found the voltage monitoring and management protocols in the plans to be robust and thorough, as they include identification of acceptable voltage limits, and processes and provisions for voltage control.

All of the transmission operator participants' restoration plans include energization guidelines for operators to limit the impact of sustained high voltages and switching transients during restoration, based on the unique characteristics of their systems.[38] Some participants' plans require that their operators connect load to newly-energized paths prior to energizing additional higher nominal voltage lines, and have a minimum loading requirement per mile of transmission line for energizing these higher nominal voltage lines (e.g., EHV transmission lines). Other participants' plans avoid energizing higher nominal voltage transmission lines early in the restoration process due to their excessive reactive requirements.

Participants that plan to energize higher nominal voltage transmission lines early in the restoration process manage overvoltage risk by placing shunt reactors or static VAr compensators in service. These participants also mitigate the risk of overvoltages by initially restoring sufficient generator capacity to provide dynamic reactive reserve. Some of the reviewed restoration plans also call for use of EHV underground transmission cables, which have a greater risk of overvoltages due to large charging currents.[39] These participants also mitigate the risk of overvoltage through the use of shunt reactors to maintain voltages within a specified bandwidth.

All participants recognized that, even when the SCADA system is available for monitoring and performing system restoration switching steps, the state estimators and real time contingency analysis (RTCA) tools typically used to analyze the impact of a transmission contingency will not be functional during system restoration.[40] When these tools are unavailable, operators are dependent on offline studies to evaluate contingencies and to identify preventative actions to ensure island stability. As discussed above in the

[38] High voltages are due to the "Ferranti effect," which is the rise in voltage resulting from energizing a transmission line that is lightly loaded. If not mitigated, this voltage increase could result in equipment damage and tripping of transmission lines.

[39] Charging currents associated with underground EHV cables can be many times greater than that of overhead transmission lines of the same nominal voltage.

[40] In the event of a large outage or blackout, these tools lack usable data inputs to function properly.

"System Restoration Resources" section, some participants' plans call for increasing operations and engineering support staffing to assist in performing off-line contingency studies that can help identify transmission contingency concerns and preventative actions when the state estimator and RTCA tools are not available. In addition, for those contingencies discovered as part of the initial assessment (e.g., impaired transmission facilities due to weather damage), participants account for this by identifying alternate or back-up facilities for system restoration, as described above in the restoration planning stages. This includes accounting for contingencies of each voltage-controlling facility on the primary restoration path (e.g. loads, shunt reactors).

c) Synchronization with Other Islands and Systems

With the initially-developed islands not connected, the islands' frequencies, voltages and phase angles must match within tolerance before interconnecting to create a merged system. Along with other factors, such as merged-system generation reserves, participants take these characteristics into account to ensure stability and avoid the risk of collapse of the merged system. To guard against collapse, participants' restoration plans identify threshold conditions that must be met prior to attempting to synchronize and interconnect separate systems. One participant determines reserves by comparing the islands' total generator capacity and island loads prior to interconnecting. In addition, some participants study contingencies (e.g., loss of largest generator) prior to interconnecting to ensure the merged island will be stable.

A number of participants' restoration plans call for synchronizing to connecting systems using switching equipment at generating stations. This approach has several advantages. First, operating personnel at generating stations perform synchronizing on a routine basis and are therefore very familiar with the process. Moreover, adjustment of the frequencies and voltages is facilitated by synchronizing at generating stations.

Another participant synchronizes islands using the highest voltage line available, which allows it to take advantage of the lower impedance and higher relay loadability of the higher voltage lines. However, that participant's plan also recognizes that possible over-voltages or special considerations could prompt the use of lower voltage lines.

d) Voltage, Frequency, and Phase Angle

Prior to connecting two systems or islands, the frequencies and voltages of the two systems should ideally be close with a near-zero phase angle difference. Such exact matching will rarely if ever be feasible, and many participants have established limits for the acceptable differences in the parameters of systems being interconnected.

Participants' restoration plans typically seek to establish stabilized voltages between 90 and 110 percent of nominal voltage before attempting synchronization. As far as the acceptable voltage difference between two islands, one participant reported bringing the

two system voltages to within 2 percent of each other prior to actually tying the systems together, with the lower voltage being on the smaller system. Participants' restoration plans also call for system frequencies to be within a certain nominal range (e.g., 59.75 and 61 Hz) before attempting synchronization.

As far as the acceptable phase angle difference between two islands being connected, the restoration plans of some participants identify 30 degrees as the maximum acceptable phase angle difference between systems being connected. Other participants set synchronizing check relays to block closing the synchronizing breaker for phase angle differences in excess of 20 degrees.[41] Transmission operators coordinate with generator control operators to minimize the phase angle difference between the systems, enabling the synchronizing check relays to permit synchronizing.

e) Synchronizing Coordination

When synchronizing islands within a transmission operator's footprint, the participants' restoration plans rely on the transmission operator, who, either directly or through delegation of the tasks, authorizes operators to perform synchronizations and interconnections of internal islands with minimal involvement by the reliability coordinator.[42] The joint staff review team found that the transmission operators, transmission owners, generator operators, and generator owners generally coordinate on the formation and expansion of islands without intervention by the reliability coordinator. The joint staff review team found that these operating entities are in the best position to coordinate formation of islands and synchronization of smaller islands in the process of restoring the interconnection, as they have access to all necessary information and are more frequently engaged in synchronizing operations.

When synchronizing islands between neighboring transmission operators, and in some cases when synchronizing larger islands within a transmission operator footprint, the participants' plans call for coordination by the reliability coordinator. For external transmission operator interconnections, the reliability coordinator typically validates that the conditions necessary for interconnection have been achieved. The reliability coordinator may not be able to monitor all the synchronizing parameters that are available to the system operators and field personnel (where the execution of the steps to

[41] These transmission phase angle settings are based on engineering analysis of the specific neighboring areas to protect against instability upon closing the breaker.

[42] As conditions permit, these islands will be formed and interconnected in accordance with the restoration plan, modified as required by system conditions.

synchronize is performed). However, the reliability coordinator will monitor the evolving restoration effort, using its wide area view capability, and can identify interconnection synchronizing opportunities not necessarily apparent to the individual transmission operators. In these circumstances, the reliability coordinator may instruct a transmission operator to interconnect.

The joint staff review team found that having the reliability coordinator coordinate inter-transmission operator interconnections has several advantages. The reliability coordinator can include in the Reliability Coordinator Area Restoration Plan specific, well thought out procedures to ensure a uniform approach to synchronization throughout the reliability coordinator's area. The reliability coordinator can then ensure that all the steps in the process have been carefully performed prior to any interconnection operation being attempted. This step is critical when interconnecting areas are in different transmission operator footprints. These will typically be large interconnections, and the consequences of a failed interconnection attempt, such as the loss of both islands, are apt to be severe. Placing such interconnections under the authority of the reliability coordinator better ensures that entities have undertaken all preliminary steps, and that the interconnection will be successful.

Some participants include standard forms and procedures in their restoration plans to guide system operators performing the interconnection of islands. Some participants' plans identify specific islands to be formed, specific synchronizing points to be used, and synchronization parameters. Others include narrative guidance for preparing to synchronize, and forms to be used during the synchronizing process. These forms typically identify those system parameters that the system operator is expected to consider before commencing the synchronizing process. All involved system operators are expected to complete these worksheets and to analyze the system parameters to determine if they are within entity limits before proceeding. Participants train on restoration synchronization in their training programs and drills. Some participants also emphasize synchronization training during regional training exercises.

3. Related Standards Assessment

Several of the sub-requirements of Reliability Standard EOP-005-2 specify elements that an entity must include in its restoration plan, many of which relate to the island development and synchronization topics discussed above. The relevant sub-requirements require the restoration plan to include:

> **R1.3.** Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.
>
> . . .

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

As a general matter, the joint team found the relevant Requirements to be sufficiently detailed and specific as to the elements that must be included in a restoration plan related to island development and synchronization. Moreover, the overall viability of the plan, including its approach to island development and synchronization, is tested through simulation testing and is reviewed and approved by the reliability coordinator. With respect to identifying cranking paths and initial switching requirements (Requirement R1.5), the joint staff review team found that the participants' plans and procedures have highly-detailed switching steps and a range of resources for reliable restoration, such as back-up cranking paths. As described earlier, the joint team found that participants are well-prepared for the unavailability of primary restoration paths, by, among other things, identifying and planning for the use of back-up paths.

The team also found that the participants' plans include applicable voltage limits during restoration, and otherwise cover the provision of voltage control in great detail. Participants' plans include identification of acceptable voltage and frequency limits and processes for restoring loads needed for restoration (such as station service for substations, load needed to stabilize generation and frequency, generating units to be started or stabilized, and detailed provisions for voltage control). Similarly, the joint staff review team found that the participants' plans have detailed procedures for restoration, reconnection and synchronization that also reflect the impact of contingencies (such as instability and loss of transmission) on voltage and frequency, on availability of reserves, and on synchronization.

As noted above, the team found that the participants' restoration plans incorporate some level of planning for contingencies (*e.g.*, by identifying and planning for the use of back-up cranking paths). However, the joint staff review team recommends tightening the requirements to modify restoration plans to reflect changed circumstances. For example, a given cranking or restoration path may be modified, which could change the

implementation of a restoration plan. Reliability Standard EOP-005-2, Requirement R4 requires:

> **R4.** Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan.
>
> **R4.1** Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

The standard as currently written does not require updates to the restoration plan for non-permanent unplanned system modifications, even when they may be long-term and affect implementation of a given entity's restoration plan.[43]

Given the critical nature of identifying and planning for the use of restoration paths to the success of the restoration plan, the joint staff review team concludes there is a need for updating restoration plans for system modifications that would change implementation of an entity's restoration plan for an extended period of time. While the joint staff review team recognizes that restoration plans necessarily incorporate some degree of flexibility so that they need not be updated with every change in configuration, the Reliability Standards do not currently require for instance, any update for an unplanned, but not permanent, system modification, regardless of whether the restoration plan is sufficiently flexible to address that change in system configuration. For example, if a transmission operator determines that an extended outage of a generator changes the implementation of the restoration plan, then the plan should be updated. Notably, the team found that some participants currently update their plans when, for example, there is a modification to a cranking path that changes their restoration plan.

4. Recommendations

Clarify when system changes will trigger a requirement to update restora

The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address the need for updating restoration plans for all system modifications that would change the implementation of an entity's restoration plan for an extended period of time, not just permanent or planned system

[43] When the IERP reviewed this requirement, it recommended requiring entities to update their restoration plan for *all* system changes that impact an entity's plan for an extended period of time (not just permanent system changes). IERP Scoring Sheet at cell S594.

modifications. In considering measures, the kinds of events that may warrant an update to the system restoration plan should be identified, taking into account the length of time the system is affected, as well as the overall objective of ensuring that restoration plans are generally flexible enough so that system modifications can be addressed without frequent updates.

5. Observed Practices for Consideration

In evaluating each participant's island development and synchronization related procedures, the joint staff review team observed the following practices and recommends consideration of these by entities:

- Many of the participants' restoration procedures require identification of back-up or alternate cranking paths during a forced or planned outage of the restoration plan-identified cranking path or segment of the path.

- Some participants include in their restoration plans the use of illustrations and accompanying steps to assist operators in system restoration, which the joint staff review team found to be a valuable aid to the operators in execution of the plan. The types of illustrations and guidelines include: electrical (i.e., one-line) diagrams, and tables or chart of reference information to augment the steps of restoration.

- Some participants include in their restoration plans a summary preceding each section of blackstart cranking path switching procedures, which participants indicated was very helpful to operators during island development.

- Some participants include in their restoration plans load pickup curves or data tables which help operators in planning the amount of online generator capacity needed to ensure island stability.

- Some participants account for seasonality when calculating cold load pickup values.

- Some participants include in their restoration plans multiple, diversely located frequency measurement sources to assist operators during system restoration, as well as in detection of an islanded condition.

- Some participants use island data monitoring methods and tools to manage island development (i.e., methods and tools to monitor frequency, voltage, load and reserves) during system restoration. These tools are used to calculate whether there is enough generating capacity online for the next increment of load pickup, and for evaluating the contingency loss of the largest island generator, as well as

in preparation to transition to balancing authority control in the later stages of restoration.

- Some participants incorporate transmission line charging current/MVAr tables into their restoration plans (to help operators in their attempts to balance reactive requirements on transmission lines using line charging so that voltages can be maintained within limits).

- Some participants prioritize the restoration of power to pumps that maintain oil pressure on underground cables used during the restoration process, to maintain the dielectric strength of the cables and to prevent failure of the cables during restoration.

- Some participants include in their restoration plans a checklist for transitioning to balancing authority control, which can be used to track the necessary details for the transfer, such as online generator attributes (capacity, control mode, output, and restrictions), current and forecasted load values, reserve positions, reconnected tie-lines with neighboring transmission operator(s), etc.

F. Testing of System Restoration Resources

1. Summary

The joint staff review team examined the participants' testing of system restoration resources, including blackstart resources and communications and control center resources, under their respective restoration plans.

As described in detail below, the joint staff review team found that all of the participants test their system restoration resources in accordance with the current Reliability Standards, and some participants have testing requirements and procedures that exceed the standards, such as energizing a blackstart unit's cranking path and starting the next unit. The review team recommends a study be performed to identify options for expanding the testing of blackstart resources to ensure they can energize equipment needed to restore the system as intended in the restoration plan, including consideration of whether such testing is practical while maintaining system reliability, and whether such expanded testing requirements could affect the identification of blackstart resources in the future.

2. Review of Restoration Plans

a) Actual Tests of Blackstart Resources

All of the participants' plans require periodic testing of blackstart units. Some participants test blackstart units once every three years, consistent with Reliability

Standard EOP-005-2 requirements (discussed further below), while others do so annually, exceeding the standard's requirements.

In addition, all of the participants require blackstart testing that meets the Reliability Standard's requirements with respect to the form of testing, i.e., they require a demonstration that the blackstart unit is able to start when isolated from the bulk power system and that the unit can energize a bus. Actual tests typically involve energizing the unit auxiliaries without outside power, starting the unit with the unit remaining stable (controlling voltage and frequency), then closing the generator breaker to energize a bus.

Some participants' plans include additional criteria that must be demonstrated during blackstart unit testing, including the following:

- Blackstart unit must be available to serve load within three hours;
- Blackstart unit must remain stable and control voltages while operating isolated from the grid for a period of 10-30 minutes.[44]

As mentioned above, the joint staff team observed that all participants' plans contain provisions for blackstart testing. However, the provisions do not necessarily require verification using conditions that anticipate actual blackout conditions, as some rely on simulations or on assumptions that certain equipment will be in service. The blackstart testing requirements in the Reliability Standards are limited to ensuring that a blackstart unit is functional, but they do not explicitly require verification of the ability to energize equipment under the conditions anticipated during an actual blackout situation.

Some participants test both the blackstart generator *and* cranking path energizing (not just energization of a bus), by isolating the system and supplying the cranking power to the next generating unit to be started. Participants who do this kind of testing only perform it in locations where the cranking paths can be isolated without outages to customers or other adverse impact on reliable operations. To perform these tests without loss of load, these participants must coordinate with all affected parties, including the generator operator, the transmission owner, and the transmission operator. In addition, these entities schedule the tests to minimize any associated cost and reliability impact (e.g., the blackstart unit is offline, the next generating unit to be started is offline, and system loads are at a lower level).

[44] While transmission operators are required to include a minimum duration for each test under Reliability Standard EOP-005-2, the participants' plans varied as to the minimum time specified.

The procedure for this testing is typically as follows:

- Start the blackstart unit after isolating the cranking path to the targeted unit;
- Close the blackstart unit generator breaker and energize the cranking path;
- Establish station service and start the motors and equipment needed for operating the targeted unit; and
- Close the targeted unit generator breaker and start energizing system load.

Because this type of testing requires a demonstration that the blackstart unit can establish station service and start the motors and equipment needed for the next targeted generating unit, as would be required under actual blackstart conditions, it demonstrates that the blackstart unit can and will function "as intended" under that entity's restoration plan. In addition, this type of testing can be used to benchmark against computer simulations to determine whether improvements need to be made to system restoration models or to the restoration plan procedures and/or restoration facilities and controls. Finally, this more robust testing provides an opportunity to test the coordination needed between the blackstart control room operator (i.e., the generator owner or operator), the transmission operator, and the control room operator of the next generator to be started. [45]

While the joint staff review team believes this more robust type of testing can be beneficial, as it provides a more realistic demonstration that the blackstart resource can perform as intended under the restoration plan, the team recognizes that such testing requires significant coordination in order to minimize the reliability and customer impact, and may not even be possible in certain locations, where cranking paths cannot be isolated without outages to customers. Accordingly, it may not be advisable to simply adopt a more stringent blackstart testing requirement that mimics the more robust testing currently done by some participants. Instead, the team recommends further study of the issue, including identifying other means of ensuring that the blackstart resource can function as intended, e.g. through verification of the restoration plan as a whole by analysis of actual events, steady state and dynamic simulations, or other means of testing.

[45] Close coordination by these entities can be critical to successful restoration, given that some of the priority auxiliary loads at the next generator to be started may consist of very large motors (e.g., 10,000 horsepower motors). The success of starting the next generating unit is greatly enhanced if the large motors are equipped with technologies which reduce the start-up current needed (e.g., variable frequency drives).

b) Tests of Other System Restoration Resources

The joint staff review team also observed that all of the participants' restoration plans include periodic testing and monitoring of vital communications facilities expected to be used during system restoration, in accordance with the Reliability Standards. In addition to testing of dedicated telephones or radios used for voice communications, participants' plans include periodic testing of their back-up facilities to ensure operability. Participants' plans also include testing of critical substation devices such as breakers, transformers, and protective relays. Furthermore, some participants test the functionality of various back-up voice communications facilities by having their control center staff perform normal operations occasionally using the back-up facilities, and as part of their drills.

3. Related Standards Assessment

Reliability Standard EOP-005-2 currently sets out the following requirements for blackstart resource testing, pertaining to both the frequency of testing and what must be demonstrated.

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include:

R9.1. The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2. A list of required tests including:

R9.2.1. The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2. The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

The joint staff review team found that the noted Requirements are detailed and, as described above, that the participants included the necessary testing parameters of these sub-requirements in their restoration plans. In some cases, the joint team observed that

participants exceeded the requirements, e.g., by requiring annual blackstart resource testing.[46]

The current blackstart testing requirements in Requirement R9.2 require a demonstration that such a unit can energize a bus. The provision does not go so far as to require a demonstration that the unit will be able to energize the equipment needed to start the next targeted unit.[47] Based on review of participants' actual testing as described above, the joint staff review team believes that more robust testing could be beneficial in many situations, as it would better demonstrate whether or not a blackstart resource is capable of functioning as intended by the restoration plan, i.e., whether it can start the equipment needed to start the next targeted unit in the plan, which would better mimic "real world" conditions.

The testing of other system restoration resources (non-blackstart resources) is covered by Reliability Standards other than EOP-005-2, including testing of telecommunications facilities (the Communications (COM) family of standards), control center functionality (EOP-008), and testing of protective relays (PRC-005).[48]

---

[46] While it may seem that three years could be too long of an interval, team discussions with participants revealed that there is a significant amount of planning and coordination needed to perform these tests (reliability coordinator, transmission owner, balancing authority, transmission operator, generator owner, and generator operator involvement to plan tests during low system load times, and to ensure availability of all necessary equipment, including all blackstart/cranking path resources).

[47] The IERP review of these requirements resulted in a recommendation to modify or redraft Requirement R9.2 so that it would require a demonstration of "the ability to start the unit and energize equipment under the conditions anticipated during an actual blackstart situation."

[48] Reliability Standard COM-001-1.1, R2 requires that each reliability coordinator, transmission operator, and balancing authority shall manage, alarm, test and/or actively monitor vital telecommunications facilities. Special attention shall be given to emergency telecommunications facilities and equipment not used for routine communications. Reliability Standard EOP-008-1 R1 requires each reliability coordinator, balancing authority, and transmission operator to have an operating plan describing how it will meet its functional obligations with regard to the reliable operation of the bulk electric system during loss of its primary control center functionality. In addition, EOP-008-1 R4 requires each balancing authority and transmission operator to have backup functionality that includes "monitoring, control, logging, and alarming

4. Recommendations

Blackstart resource testing under anticipated blackstart conditions. The joint staff review team recommends a study be performed to identify options for expanding restoration plan testing beyond the currently-required blackstart resource testing, to ensure the blackstart resource can energize equipment needed to restore the system as intended in the restoration plan. Any expanded testing requirements should take into consideration whether such testing is practical while maintaining system reliability, and whether such expanded testing requirements could affect the identification of blackstart resources in the future.

5. Observed Practices for Consideration

In evaluating participants' testing of system restoration resources, the joint staff review team found that some participants perform real time tests of the blackstart generator and cranking path energizing by isolating the system and supplying the cranking power to the next generating unit to be started. The joint staff review team recommends consideration of this practice by entities.

G. Testing, Verification, and Updating of System Restoration Plans

1. Summary

The joint staff review team examined the participants' plans and procedures for conducting the required testing, verification, and updating of their system restoration plans. The team examined the participants' modeling considerations and inputs, types of studies performed, study verification, simulation tools used, frequency of verification, and restoration plan completion time.

---

sufficient for maintaining compliance" with Reliability Standards that depend on a balancing authority and transmission operator's primary control center functionality. EOP-008-1 R7.2 requires an applicable entity to conduct an annual test of its operating plan that demonstrates the backup functionality, in the event that its primary control center functionality is lost, for a minimum of two continuous hours. In addition, Reliability Standard PRC-005-2(i) requires maintenance of protection systems affecting the reliability of the bulk electric system, which includes required testing of relays and other protection system components, as specified in Table 1 of the standard.

As described in detail below, the joint staff review team found that participants test their plans for viability at least every five years, in accordance with the Reliability Standards. The review team recommends that measures be taken (including considering changes to the Reliability Standards) so that plan verification through testing and simulation is performed whenever system changes occur that precipitate the need to determine whether the plan's restoration processes and procedures, when implemented, will operate reliably. In considering such measures, the types of system changes that are significant enough to warrant additional testing and verification (e.g., identification of a new blackstart generator location or on redefinition of a cranking path) should be identified, keeping in mind the overall objective of ensuring that restoration plans are flexible enough so that system changes can be addressed without frequent updates.

2. Review of Restoration Plans

a) Modeling Considerations

All of the participants' restoration plan verification methods include performing computer simulations to analyze whether their plans can accomplish the intended function. Participants employ dynamic and steady-state modeling for analyzing restoration cranking paths, as further discussed below. For accurate modeling of the cranking path loads, participants take into account auxiliary load inrush currents and auxiliary motor characteristics needed to start up the next generating unit(s). A few participants also model other load values at their predicted inrush or cold-load pickup levels, such as where large block loads are planned to be restored or used to control system voltage or frequency. Participants' models also include the dynamic characteristics of the generators needed for stability analysis.

Overall, participants' models are designed to allow for analysis of the effects of the operator switching steps to sequentially energize transmission facilities or segments, adding the expected increments of load, switching other devices in-service (such as shunt reactors), and making adjustments as necessary for island stability and operation within steady-state limits.

b) Studies and Simulations

Participants use a range of approaches to their dynamic studies, but all typically test the following:

- Viability of switching steps to energize the primary or preferred transmission cranking paths to supply the priority loads;

- Viability of switching steps to energize alternate or back-up transmission cranking paths to supply the priority loads;

- Viability of the restoration plan assuming one of the blackstart generators is not available;

- With successful blackstart cranking path power delivered and additional generators on-line, viability of switching steps to energize additional restoration paths; and

- Transient stability assuming a fault on the island system (during later stages of restoration).

Participants use dynamic simulations to ensure frequency is kept within the tolerances needed to keep generators from tripping on underfrequency. The simulations verify the capability of blackstart facilities and of other generation resources to meet real and reactive power requirements of cranking paths, and verify their dynamic capability to supply priority loads. These studies identify the location and magnitude of loads required to control voltage and frequency within acceptable operating limits.

Participants use steady state, dynamic, and contingency analysis of the system to ensure it will perform in accordance with the restoration plans. No single study will verify all aspects of a restoration plan. Participants perform their steady state and dynamic analysis using commercial power-flow software. Generally, participants run their analyses using lightly loaded cases. As mentioned above in the Island Development and Synchronization section (V.E), some participants also use seasonal cases accounting for worst-case cold load pick up values.

Steady-state Analyses. The participants use steady-state analyses to verify that steady-state voltages are maintained within limits, and to determine the real and reactive load output and voltage controlling device adjustments necessary to balance generation and load. Participants also monitor any thermal limit exceedances on transmission facilities as part of their steady-state analysis, although thermal limits during the early stages of island development are typically not as much of a concern as they are during later stages when system transfers between loads and generators increase.

Dynamic Analyses. As noted above, participants perform simulations of their plans to ensure that there are no stability issues during switching or when an event occurs. Participants commonly perform voltage analysis for the cranking path switching steps to determine any transient switching over-voltages that could result from energizing transmission lines and cables. Participants that use an EHV transmission system during the restoration process also verify the effectiveness of shunt reactors at both ends of EHV transmission lines, to ensure they can control over-voltages. The joint staff review team notes that these kinds of analyses are becoming more important as an increasing number of entities use higher-voltage cranking paths. The recent industry trend of replacing blackstart coal-fired generators which were not connected to the EHV transmission

system, with new blackstart gas-fired combustion turbine generators connected to the EHV transmission system, has increased the usage of higher voltage cranking paths.

Participants also use voltage stability analysis to verify that incremental load pickup takes cold load pickup into account, and that inrush currents do not result in voltage or generator instability. In addition, participants use voltage stability analysis to determine the generator, load, and voltage controlling device adjustments necessary to maintain acceptable voltage levels. Participants monitor frequency and voltage deviations in the analyses to prevent an element from tripping (e.g., underfrequency relay trip settings, generator low frequency limits or trip points). In an iterative manner, participants would then make any necessary adjustments to the plan to ensure acceptable voltage and frequency levels.

Some participants include testing for short circuit fault stability by imposing a simulated fault on the transmission restoration path following the initial stages of restoration to test generator stability. These N-1 simulations are generally focused on later stages of restoration because a fault during the early stage would most likely result in a generator tripping off line. As the islands grow and load is restored in their studies, these participants will run offline cases and simulate N-1 conditions.

c) Frequency of Performing Simulations

All of the participants perform their offline dynamic and steady state studies at least every five years, as required by the Reliability Standards, or more frequently if something significant changes on their system. Several participants indicated that they regularly perform their analysis on a more frequent (e.g., annual) basis.

d) Restoration Plan Completion Time

Participants indicated that estimating the time to complete a restoration plan and fully restore the system is a difficult task. Many factors must be taken into consideration, including the extent of the blackout, damage to the system, state of generating units and the system status of neighboring utilities. Participants' restoration plans are designed on the assumption of a total blackout with no help from their neighbors. For those participants that do incorporate a target restoration time into their restoration plans, the estimates on restoring the transmission operator's system range from as few as seven hours to as many as 16 hours. However, these estimates assume that all goes according to plan and few issues arise during restoration. Most participants have encountered longer restoration times during simulations.

Some participants factor these potentially lengthy restoration times into the sizing of station batteries, which are considered to be vital resources during system restoration since they provide power to station equipment when system power is lost. As discussed earlier in the System Restoration Resources section (Section IV.D), some participants

size batteries to provide power for a longer time (e.g., 24 hours) for certain substations that are a priority for restoration, for more remote stations, or where the participant anticipates difficulty reaching the station due to damage from a natural disaster (e.g. areas more prone to hurricane weather). Portable batteries and portable generators are also employed to supply station power if needed during restoration. Some participants also install local generation at key facilities as back-up power sources and test these generators regularly to ensure operability.

3. Related Standards Assessment

Requirement R6 of Reliability Standard EOP-005-2 requires transmission operators to verify that their restoration plan can accomplish its "intended function" through analysis of actual events, simulations, and testing, and sets out specific capabilities that must be confirmed:

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify:

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

The joint staff review team found that the noted Requirements are sufficiently detailed, noting that the accuracy of the simulations and models are influenced by the Requirements of Reliability Standard TPL-001-4, assessment modeling, and related system modeling (MOD) standards to ensure their restoration plans are viable in the event of an actual blackout. These requirements, taken collectively, would ensure sufficiency and expose any inadequacies of a bare-bones or inaccurate model. In addition, the joint staff review team found that participants perform extensive steady-state and dynamic simulations, including short-circuit fault stability analyses in some cases, to test whether the blackstart resources can meet the requirements to supply initial loads (R6.1), and to verify the capability of loads and generating resources to ensure voltages and frequency are kept within acceptable limits (EOP-005-2 R6.2 and R6.3). However, the team identified one concern with the scope of Requirement R6 of this standard: transmission operators are required to verify the effectiveness of their restoration plan

every five years, but are not required to perform additional simulations or testing if their restoration plan is impacted by a change.[49] For example, given recent changes occurring with blackstart resources (as described earlier in the report), the joint staff review team is concerned that many entities may have to modify their restoration plans going forward, but may not verify that the modified plan can accomplish its intended function until as late as five years after making the change.

While the reliability goal is for transmission operators to have up-to-date and verified restoration plans, the joint staff review team recognizes that the triggers for re-verification of the plan should be clearly set out, and that re-verification of the full plan may not be necessary in all situations where a restoration plan has been or should be updated. For example, the addition of new blackstart generation or redefinition of a cranking path may warrant additional verification, but it may not necessitate computer stability simulations of other areas of the plan. At a minimum, however, re-verification should occur when needed to ensure that the restoration plan can, when implemented, allow for restoration of the system within acceptable operating voltage and frequency limits.[50]

4. Recommendation

Verification/testing of modified restoration plan. The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards)s to address the need for re-verification of a system restoration plan when a system change precipitates the need to determine whether the plan's restoration processes and procedures, when implemented, will operate reliably; i.e., when needed to ensure that the restoration plan, when implemented, allows for restoration of the system within acceptable operating voltage and frequency limits. In considering and developing such measures, the types of system changes that could impact reliable implementation of the restoration plan should be taken into account (e.g., identification of a new blackstart generator or on redefinition of a cranking path).

[49] The joint staff review team recognizes that the Reliability Standard EOP-005-2, Requirement R4 currently addresses the need to update restoration plans given a planned system modification that would change the implementation of the plan, but does not require a re-verification of the plan's effectiveness following the modification.

[50] *See* Section IV.E Island Development and Synchronization.

5. Observed Practices for Consideration

Due to the potential length of the restoration process, some participants size batteries to provide power for a relatively long time (e.g., 24 hours) for certain substations that are a priority for restoration, for more remote stations, or where the participant anticipates difficulty reaching the station due to damage from a natural disaster (e.g. areas more prone to hurricane weather). Portable batteries and portable generators are also employed to supply station power if needed during restoration. Some participants also install local generation at key facilities as back-up power sources and test these generators regularly to ensure operability. The joint staff review team recommends consideration of these practices by entities.

H. System Restoration Drills and Training Exercises

1. Summary

The joint staff review team examined the participants' plans and procedures for conducting system restoration drills and training exercises, and observed some of the participants' actual system restoration exercises. The joint staff review team observed that the participants' restoration plans address restoration plan training and drilling, including training on coordination with other entities, restoration priorities, building cranking paths and synchronizing to the interconnection.

However, the joint staff review team found that participants' plans are not clear regarding training on the processes for transfer of control from transmission operator to balancing authority during system restoration. This transfer of control is a crucial step in the restoration process and can require coordination between several entities. Therefore, the joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address drills and training on the operating processes for transferring authority from the transmission operator back to the balancing authority. These measures would allow transmission operators, reliability coordinators, and relevant generator operators to gain experience on the coordination needed through all the stages of restoration, including coordination needed in the transfer of control back to the balancing authority.

2. Review of Restoration Plans

The joint staff review team found that participants' system restoration drills facilitate the review of their system restoration plans and emergency operating procedures, and provide coordinated training for operators through simulation exercises. Participants use restoration drills to review and understand their (and other entities') plans, to coordinate with neighboring entities, to identify weaknesses in restoration plans while identifying ways to improve them, to verify results of system studies pertaining to restoration, and to maintain familiarity with established processes. Depending on the sponsor, system

restoration drills may include reliability coordinators, transmission operators, generator operators, and in some areas, certain transmission and generator owners. By promoting regional coordination between entities, participants' system restoration drills provide greater regional exposure for operators, promote sharing of knowledge and lessons learned among system operators, and can improve future interaction between entities.

As discussed further below, the joint staff review team found that the system restoration drills allow for coordinated training of operators using simulation exercises, and also test the interaction between operating entities during the execution of their system restoration plans. These drills require interaction between neighboring entities, which mimics the required response to a real-life event and promotes better communications and cooperation among neighboring entities. The drills also facilitate the development of the skills, experience and tools required to effectively manage the system restoration process. In general, the drills are designed to improve system operator skills and prepare them to efficiently respond to rare, catastrophic events such as a partial or total shutdown of the bulk power system. The drills also require interactions between entities that do not routinely work together that may have to cooperate to remedy a blackout.

The joint staff review team also found that execution of organized periodic system restoration drills provides the participants a mechanism by which any weaknesses or defects in the restoration plan may be exposed. The periodic drills, along with associated debriefs and operator feedback, facilitate the evaluation of existing restoration methods and provide an opportunity for continuous improvement. Because Reliability Standard EOP-005-2 Requirement R10 mandates annual system restoration training for all system operators, it is likely that on-duty operators will have been trained prior to having to implement the plan during an actual restoration event.

a) Planning a Restoration Drill

Participants indicated that some of the drill exercises are sponsored and developed at the reliability coordinator level. These drills are developed in collaboration with drill coordinators and operators from the reliability coordinator, transmission operators, generator operators, and certain transmission owners who perform restoration steps in accordance with the transmission operators' restoration plans. The joint staff review team found that a reliability coordinator-sponsored system restoration drill is normally planned several months prior to the actual drill. During annual training, a reliability coordinator typically schedules training sessions to prepare operators for specific topics related to system restoration. Similarly, system restoration drills sponsored at the transmission operator level are planned in advance, and operating personnel are trained on the system restoration procedures prior to the drill.

The joint staff review team observed that generally, prior to finalizing drill scenarios, details of the simulated event are reviewed by the coordinators of participating entities to identify potential opportunities for interacting with neighboring entities, and to resolve

issues that may adversely impact the execution of the drill. A final system restoration drill plan is then provided to participating entities, which typically includes the following:

- Scope of the drill – initial condition of the interconnection from which the operators intend to execute their plans, including information regarding whether the drill involves a total or partial shutdown of the interconnection.

- Checklist of information (restoration tracking form) to be completed by the participants and passed on to the drill sponsor – generation and transmission facility information is used to record and track equipment status and to provide updates on restoration progress to the drill sponsor.

- "Injects" or specific unexpected constraints to be included by the drill sponsor to mimic possible failures of equipment or issues that may impact the restoration process - injects can include the loss or unavailability of major transmission lines, other transmission equipment, cranking paths, generation, or substations. Injects can also include factors such as loss or impairment of communication with field personnel or the loss of battery power at a substation.

Review of participants' plans and other procedures showed that the participants typically conduct or otherwise participate in restoration drills during the spring and fall each year (during lower load periods of the year). This affords greater availability of operators to dedicate to the restoration training. For some drills, blackstart generator operators and other generator operators needed for the restoration plans are invited to participate. Some participants indicated that, in their experience, involving these generator operators makes the drill more realistic and provides valuable collaborative experience for all participants.

b) Training Scenarios and Exercise Tools

Some participants undertake training drills more frequently than is required by the Reliability Standards, in order to allow for the use of different outage scenarios, or initial conditions, for each drill. These scenarios and initial conditions include, but are not limited to:

- Entire blackout of a region encompassing multiple entities;

- Partial blackout of a region, with separation into electrical islands within the region; and

- Regional blackout, with a cyber impact condition, resulting in loss of tools such as SCADA for some entities.

The drills conducted by participants also typically cover operator roles and responsibilities, and plans for communications.

Operator Training Simulators. The joint review team found that most participants use operator or dispatcher training simulators (DTS) to provide computer simulations of system restoration drills. In many applications, the DTS allows the participating operators to use the same tools and computer applications used in normal operations for the many steps executed during system restoration. The DTS system also tracks the status of generation and dynamically updates and displays the latest simulated system conditions. Moreover, accuracy of simulations to the actual system is created by building DTS systems from snapshots of actual system conditions accessed from the entity's SCADA system.

Participants also use tabletop exercises during which operating personnel discuss, in an informal setting, the effectiveness of their restoration plans, policies, and procedures under various possible scenarios, and the expected restoration steps to take. Some tabletop exercises also involve drilling on communications and coordination between operators (e.g., operators located at separate training facilities). The joint staff review team found that the structure of a tabletop exercise allows for open discussion among participants. However, tabletop exercises do not provide the full simulation experience possible with an operator training simulator, where the computer simulations for operator-execution of the restoration plan steps provide a more realistic experience.

Communications Tools. The joint staff review team found that during the early stages of restoration drills, participants typically test their primary and back-up communications systems, including telephones and other systems used for messaging. Participants send and receive messages and information via email, telephone, or facsimile (fax) during restoration drills, i.e. using the same media that would be used during a system emergency. The joint staff review team found that the communications tools provide an effective way for the participants to communicate with neighboring entities and to send summaries of the status of their restoration to the reliability coordinator or transmission operator, as well as providing the reliability coordinator or transmission operator a means to provide notification or feedback to participants. The drills may also exercise communications tools normally reserved for emergency situations, thus improving familiarity with these systems.

Restoration Maps and Tracking Forms. In most of the training drills observed by the joint staff review team, the sponsoring entity (in that case, the reliability coordinator) provided participants with a restoration tracking form as described above. As the system restoration drill progressed, the participants provided updated information to the reliability coordinator using the tracking forms, and the reliability coordinator updated its

system models with the latest information as provided by participants.[51] In addition to restoration tracking forms, participants use as part of the restoration training and drilling process restoration maps, which geographically illustrate the location of substations, generation and interconnected transmission. Maps also show opportunities for connecting neighboring systems, voltage class, and lines out of service. Some participants use electronic maps, which are updated as information is received from other participants. In these cases, information received is processed and linked to the map on a periodic basis (e.g., within an hour). Other participants overlay restored lines on a geographic map board.

c) Drill Observations

As noted above, the joint staff review team observed system restoration exercises in which some of the participants took part. In the observed drills, the reliability coordinators initially focused on coordinating the restoration of offsite power to nuclear generating units for safe shutdown. This effort included transmission operators identifying blackstart units within their footprints and coordinating with the reliability coordinator to deliver power to nuclear generating units via specified transmission paths. The observed drills also included scenarios that involved coordination of such offsite power supply from outside a participating transmission operator's footprint, using pre-established plans that could involve multiple adjacent transmission operators.

During reliability coordinator-sponsored drills, the team observed several conference calls between staff of the reliability coordinator and transmission operators, which allowed the transmission operators to discuss outstanding issues or obstacles faced in the restoration process with the reliability coordinator. In addition, the team observed that the reliability coordinators make open party communication lines available to all participating transmission operators during the restoration drills.

During the mid-stage of observed drills, some participating transmission operators were able to connect islands within their respective footprints, connect to external islands outside of the reliability coordinator's footprint, or connect to other islands within the reliability coordinator's footprint with approval from the reliability coordinator. The

[51] The tracked information can include information on blackstart resources providing offsite power to nuclear units, the largest contingency in a particular island, amount of load restored, power available in a particular transmission operator's island or footprint, dynamic reserves available in each island, number of islands for each transmission operator, and tie line schedules and locations for synchronization with other transmission operators.

team also observed that the reliability coordinator operators usually recommend which ties to begin connecting between the transmission operators, based on system topography and proximity to stable external power.

During some of the observed restoration drills, the reliability coordinator focused on restoring the high voltage transmission system or "backbone" transmission early in the restoration process, using multiple cranking paths, and then coordinated the delivery of offsite power to nuclear units for safe shutdown. Next, the transmission operators used power from the "backbone" transmission to power islands created within their footprints. These system restoration drills used a "top-down" approach, since participating transmission operators used power from the "backbone" to restore their respective areas.

Generally, for transmission operator-sponsored drills, the transmission operator monitors island frequency, voltage and VArs as drills progress, using computer displays of SCADA data. The team observed transmission operators coordinating generation start up to regulate island frequency and switching of reactive components to maintain voltage and VArs in the islands created. In certain situations, neighboring transmission operators connected adjacent islands, thereby establishing larger islands. After multiple larger islands were created, more opportunities to simulate synchronization with other adjacent islands or external stable interconnections were identified.

Generally, at the conclusion of the observed system restoration drills, participating reliability coordinators and transmission operators requested and received feedback from drill participants. The transmission operators typically report any deficiencies found in their restoration plans during the drill to the reliability coordinator and subsequently seek to correct those deficiencies. Both reliability coordinators and transmission operators typically review the feedback provided by the participating entities to inform future system restoration drills and improve existing restoration plans. For example, as feedback, participating transmission operators in one observed drill reported issues with their blackstart plans, simulator issues, and coordination issues with other transmission operators.

The joint staff review team identified one area for improvement through its observation of these various drills and training scenarios, finding that in some instances, the process for transferring control of generation back to the balancing authority was not focused on as part of the drill.

3. Related Standards Assessment

Reliability Standard EOP-005-2 currently sets out explicit requirements for system restoration training and drills, including what must be demonstrated. Requirement R10 of EOP-005-2 requires each transmission operator to conduct annual system restoration training for its system operators, including training on specific areas, as follows:

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following:

R10.1 System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2 Restoration priorities.

R10.3 Building of cranking paths.

R10.4 Synchronizing (re-energized sections of the System).

In addition, Requirements R12 and R18 of Reliability Standard EOP-005-2 require transmission operators and generator operators to take part in their reliability coordinator's restoration training drills and exercises:

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator.

The joint staff review team found that the training-related requirements (R10, including R10.1-R10.4) of the Reliability Standard are clear and effective. Participants' restoration plans, training procedures and scenarios extensively cover the coordination and exercising of the steps of restoration identified in these requirements. However, the team concludes from its review and discussion with participants that training on the criteria and steps for the transfer of control from the transmission operator back to the balancing authority during the late stages of restoration may not be sufficient. Some of the concern regarding the lack of training in this area may be attributable to the lack of guidance in some participants' plans regarding the initiating factors, methods and permissions for this important transfer. The joint team also observed that exercises related to the transfer of control from the transmission operator to the balancing authority are usually planned for the latter part of the training sessions. Therefore, exercises may not be implemented sufficiently to train operators on these topics. Thus, the joint staff review team recommends considering revisions to the Reliability Standards to require training focused on the transfer of control from transmission operators to the balancing authority.

Reliability Standard EOP-005-2, Requirements R12 and R18 require that each transmission operator and generator operator participate in its reliability coordinator's

restoration drills, exercises or simulations as requested by its reliability coordinator. The joint staff review team did not identify any clarity or efficacy concerns with these requirements, or any other concerns, except as described above, with generator operators' or transmission operators' actual participation in reliability coordinator-convened restoration drills and training.

4. Recommendations

Operator training: exercises on transferring control back to balancing aut

The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address system restoration training and drilling for transitioning from transmission operator island control to balancing authority ACE/AGC control. These measures will allow transmission operators, reliability coordinators, and relevant generator operators to gain experience on the coordination needed through all the stages of restoration, including coordination needed in the transfer of control back to the balancing authority.

5. Observed Practices for Consideration

In evaluating participants' system restoration drills and training exercises, the joint staff review team observed the following practices and recommends consideration of these by entities:

- Most participants use operator or dispatcher training simulators (DTS) to provide computer simulations of system restoration drills. In many applications, the DTS allows the participating operators to use the same tools and computer applications used in normal operations for the many steps executed during system restoration. The DTS system also tracks the status of generation and dynamically updates and displays the latest simulated system conditions.

- Some participants use unexpected scenarios and added visualization as part of participants' restoration training and drilling process, which included the following:

    - Constraints (injects) to mimic possible failures of certain equipment or existing system issues that may impact the restoration process.

    - The use of electronic maps that update dynamically and provide the most up-to-date visual display of the restored system to operators.

I. Incorporating Lessons Learned from Prior Outage Events

1. Summary

The joint staff review team examined the extent to which lessons learned from major outage events are incorporated in the restoration plans of the review participants. The review team examined recommendations from:

- 2011 Arizona-Southern California Outages,
- Hurricanes Gustav (2008) and Sandy (2012), and
- 2011 Cold Snap and 2014 Polar Vortex.

The joint staff review team observed that all participants incorporate the analysis of actual outage events through review of recommendations and lessons learned to enhance their restoration plan procedures. The team found that this practice helps to ensure the viability of the participants' restoration plans, and that the relevant Reliability Standards addressing the analysis of actual events are clear and effective. With the understanding that some areas have never experienced a blackout, the team recommends that applicable entities that have not experienced a blackout or other events which impacted, or could have the potential to impact, the viability of their restoration plans reach out to those who have, in order to gain more knowledge on improving their own restoration plans.

2. Reports from Recent Events

a) 2011 Arizona-Southern California Outages

On September 8, 2011, a disturbance occurred in the Southwest, leading to cascading outages and approximately 2.7 million customers without power. The outages affected parts of Arizona, Southern California, and Baja California, Mexico. All of the San Diego area lost power, with nearly one-and-a-half million customers losing power, some for up to 12 hours.[52]

The joint FERC-NERC Staff report analyzing this event made certain recommendations that pertain to the restoration process. The report recommended that the reliability coordinator involved in that event should clarify its role, including the real-time information it can provide in emergency situations like a multi-system restoration. In addition, the report recommended that that reliability coordinator should specifically

[52] *See* FERC and NERC Staff Report, *Arizona-Southern California Outages on September 8, 2011* (April 2012) (Southwest Outage Report).

address coordination among balancing authorities and transmission operators in its operating area, outlining the areas of responsibility during system restoration and other emergencies.[53]

The joint staff review team found that participants have incorporated tables of tasks or responsibilities defining the roles, tasks, and approvals needed by each entity involved in restoration. Also, participants have identified points of contact during emergency situations dedicated to providing information. This identification of roles and responsibilities allows operators to focus on restoring the system during an emergency (see Roles, Interrelationships and Coordination section above).

b) Hurricanes Gustav (2008) and Sandy (2012)

On September 1, 2008, Hurricane Gustav made landfall in Louisiana as a strong Category 2 hurricane – 1 mph below Category 3 level. Hurricane Gustav, with impacts compared to Hurricane Katrina, resulted in outages to more than 1.3 million customers. The impacts of Gustav were concentrated primarily in Louisiana, Mississippi and Arkansas, and caused severe flooding, which slowed the restoration efforts. Moreover, due to damage to several high-voltage transmission lines, a portion of the transmission system was "islanded" during the event.[54]

On October 29, 2012, Hurricane Sandy, a Category 1 hurricane, made landfall on the New Jersey shore at around 8 p.m. Eastern time, with an unprecedented storm surge. Over the course of the event, over 8,000 MW of generation capacity was forced off line, and seven interconnections to southeastern New York, from Connecticut and New Jersey, were disconnected. By late Monday, October 29, approximately 2.2 million electric

---

[53] *See id.* at 62.

[54] *See* Infrastructure Security and Energy Restoration Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, *Comparing the Impacts of the 2005 and 2008 Hurricanes on U.S. Energy Infrastructure* 7, 9 (February, 2009). The electrical island was first detected by operator-monitoring of PMUs installed across Mississippi, Louisiana, Arkansas and East Texas, where operators were alerted to the island's creation by the diverging system frequencies. The electrical island existed for approximately 33 hours, until transmission facilities were restored and re-synchronization with the Eastern Interconnection occurred. *See* Kolluri, S.; Mandal, S.; Galvan, F.; Thomas, M., *The Role of Phasor Data in Emergency Operations*, Transmission T&D World Magazine (Dec. 1, 2008), and Power & Energy Society General Meeting, 2009. PES '09. IEEE, doi: 10.1109/PES.2009.5275340, 1, 5, and 26-30 (July 2009).

customer outages were reported. The storm surge was so extensive that transmission owners reported that low-lying stations were flooded to the degree that staff had to evacuate for safety reasons.[55]

With respect to Gustav, the use of PMUs from multiple transmission substations to monitor system frequency at diverse locations aided in island monitoring and management of load pick-up, and in detection of an islanded condition. Lessons learned from Sandy included the value of tracking the *combined* effects of tides and storm surge, and in increased operator awareness that storm surge projections became accurate only within one day of the storm.

The joint staff review team found through participant discussions, on-site observations and reviews of emergency response and restoration plans regarding these and other similar recent events (e.g., Hurricane Katrina in 2005), that participants more prone to severe coastal weather patterns and associated damage have incorporated several lessons learned from those events. These lessons include maintaining large inventories of transmission line and substation equipment, along with establishing storm response plans for closely monitoring forecasted weather conditions, mobilizing equipment, and for activating operations and field personnel to expedite restoration.[56]

---

[55] System impacts included outages to 28 345 kV transmission lines, one 230 kV transmission line, 42 138 kV transmission lines, and 15 115 kV transmission lines. Generating facilities over a very wide footprint were forced off line. Some generators were rendered unavailable due to the loss of interconnecting transmission. There were also reports of other generators that were forced into preemptive "shut-downs" to protect assets from long-term damage or for human safety reasons. *See* New York Independent System Operator, *Hurricane Sandy: A report from the New York Independent System Operator* (March 2013), http://www.nysrc.org/pdf/MeetingMaterial/RCMSMeetingMaterial/RCMS%20Agenda%20159/Sandy_Report___3_27_133.pdf.

[56] While beyond the scope of this report, the possibility of damage to major equipment has been discussed in reports by various others, such as the National Research Council of the National Academies, "Terrorism and the Electric Power Delivery System," 69-91 (2012) (focusing on transmission towers, mobile generators and transformers and shared inventories of transformers); Department of Energy, "Large Power Transformers and the U.S. Electric Grid Report," (2012, updated in 2014); Center for the Study of the Presidency & Congress, "Securing the U.S. Electrical Grid," (2014) (citing mutual assistance agreements and shared inventories for equipment such as transformers); and

c) 2011 Cold Snap and 2014 Polar Vortex

During the first week of February 2011, the southwest region of the United States experienced unusually cold and windy weather, with lows in the teens for five consecutive mornings and many sustained hours of below freezing temperatures throughout Texas and in New Mexico. Between February 1 and February 4, 2011 individual generating units throughout Texas experienced either an outage, a derate, or a failure to start. These reductions in available generation were severe enough to trigger a controlled load shed of 4,000 MW. In total, 4.4 million customers were affected over the course of the event.[57]

In early January 2014, the Midwest, South Central and East Coast regions of the United States experienced a polar vortex, where some areas were 35° F or more below their average temperatures, resulting in record high electrical demand. One of the largest issues affecting gas-fired generators during the polar vortex was the curtailment or interruption of fuel supply. Extreme cold weather also had a major impact on generator equipment. Of the approximately 19,500 MW of generator capacity lost due to cold weather, over 17,700 MW was due to frozen equipment. [58]

NERC, "Severe Impact Resilience: Considerations and Recommendations," 50-51 (2012).

[57] System operators initiated controlled rolling blackouts during the event. Although emergency conditions existed, entities' restoration plans did not need to be deployed. Had a total blackout occurred in the region, the unavailability of 10 blackstart resources, comprising 687 MW out of a total 1150 MW of blackstart capacity, could have jeopardized the ability to promptly restore the system. *See Report on Outages and Curtailments During the Southwest Cold Weather Event of February 1-5, 2011* (August 2011), http://www.ferc.gov/legal/staff-reports/08-16-11-report.pdf (2011 Cold Snap Report).

[58] Many generator outages, including a number of those in the southeastern United States, were the result of temperatures that fell below the plant's design basis for cold weather. At the height of generation outages (January 7, 2014 at 0800 Eastern time), the southeastern United States accounted for approximately 9,800 MW of the outages attributed to cold weather. While widespread outages occurred, no blackouts occurred and system operators were able to successfully maintain reliability. *See* North American Electric Reliability Corp., *Polar Vortex Review*, at iv, 2, 19 (Sept. 2014).

One recommendation from the 2011 Cold Snap Report pertains to system restoration, advising that balancing authorities, transmission operators and generator owners/operators take the steps necessary to ensure that blackstart generators can be utilized during adverse weather and emergency conditions.[59]

The joint staff review team found during its review that participants do not typically test blackstart units during extreme temperatures. Many blackstart resources are needed as peaking generators during times of high demand, and entities commonly do not risk scheduling a test during these periods. However, other lessons learned have been incorporated in participants' restoration planning, including implementing weather–related emergency procedures which include alert levels and triggers. These procedures include steps for requesting additional generator reserves, including the distribution or location of additional reserves (through means such as adjusting reserve requirements), as well as the cancelling of upcoming maintenance or limiting planned outages to enhance more operational flexibility during the storm or possible severe weather periods.

3. Related Standards Assessment

Reliability Standard EOP-005-2, Requirement R6 requires transmission operators to verify the functionality of their restoration plan based on actual events, among other things:

> **R6.** Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function . . . .

Based on the joint staff review of participants' analyses of actual events, no related clarity or efficacy concerns were identified. The joint staff review team found that participants routinely review lessons learned from events such as those above, and similar weather events (e.g., Hurricane Katrina), and incorporate them into their emergency response and restoration plans where applicable, recognizing there is no substitute for experience. The incorporation of lessons learned from actual events into these plans is mostly done on an intra-regional basis through restoration working groups. The joint team learned that some participants at the ISO level regularly share experiences and lessons learned from drills with ISOs from adjacent regions, which these participants found beneficial.

[59] Recommendation 7 from the 2011 Cold Snap Report.

4. Recommendations

Obtaining insight from entities that have experienced a widespread outag The joint staff review team found that participants place the utmost importance on past experiences and lessons learned from events, including the lessons learned from historical blackouts and other significant events related to the viability of restoration plans, and currently share information through restoration working groups and other means. However, the team is concerned that entities that have not experienced blackout conditions may not be fully aware of all the additional insight and lessons learned by entities that have experienced significant blackouts, particularly for blackouts and events in other regions. Therefore, the team recommends that applicable entities that have not recently experienced a blackout or other event which impacted, or could have the potential to impact, the viability of their restoration plans reach out to those who have experienced such events, in an effort to continually improve their restoration plans. Entities could benefit from the sharing of experiences across different regions of the country to gain insight into events that may not have occurred locally within a region, including but not limited to:

- Severe flooding and storm impacts on facilities and equipment depended on for system restoration;
- Effects of extreme temperatures, including severe cold weather impacts on facilities and equipment depended on for system restoration; and
- Preparedness training for the above impacts.

5. Observed Practices for Consideration

The joint staff review team found that lessons learned from past major events have been incorporated into participants' emergency response plans and restoration plans where applicable. The joint staff review team observed the following practices and recommends consideration of these by other entities:

- Use of diversely-located frequency measurements, e.g., PMUs for system operator monitoring of frequency (*see* Island Development and Synchronization section above).
- Maintaining large inventories of transmission line and substation equipment, along with establishing storm response plans, closely monitoring forecasted weather conditions, mobilizing equipment, and activating operations and field personnel to expedite restoration (*see* Island Development and Synchronization section above).

- Developing and implementing extreme weather–related procedures, including alert levels and triggers to initiate the request for additional generator reserves, including the distribution or location of additional reserves (through means such as adjusting reserve requirements). Such procedures could also include cancelling upcoming maintenance or limiting planned outages to enhance operational flexibility during severe weather periods.

- Assigning roles and responsibilities across operator desks during system restoration, as well as identifying points of contact during emergency situations dedicated to providing information. This identification of roles and responsibilities allows operators to focus on restoring the system during an emergency.

- Several participants indicated that lessons learned can be sourced from smaller events just as much as from the larger events, and that sharing and analysis of these events can be accomplished, for example, through the ERO Events Analysis Process.[60]

V. Review of Cyber Security Incident Response and Recovery Plans and Related Standards Assessment

The joint staff review team reliability assessment also included review of cyber security incident response plans and recovery plans for critical cyber assets, along with associated procedures and resources of the participants, to assess their readiness to respond and recover in the event of a cyber security event. This report provides a breakdown of the review by various response and recovery topics. These topics include:

- Resources, Processes, and Tools for Cyber Incident Response and Recovery;

- External Roles, Interrelationships and Coordination;

- Monitoring for and Detection of Cyber Incidents and Triggers for Incident Response;

- Initial Event Response Actions;

[60] See http://www.nerc.com/pa/rrm/ea/Pages/EA-Program.aspx.

- Recovery Planning;
- Review and Verification of Incident Response and Recovery Plans;
- Drills and Training Exercises; and
- Improving Cyber Security Response and Recovery Plans Based on Actual Events and Other Feedback.

As noted above, included at the close of each topic is an analysis of the participants' plans against the relevant Critical Infrastructure Protection (CIP) Reliability Standards, to see where improvements in the clarity or efficacy of the standard may be warranted.

A. Resources, Processes, and Tools for Cyber Incident Response an Recovery

1. Summary

The joint staff review team examined the resources, processes, and tools participants plan to deploy in responding to cyber incidents and in recovery of critical cyber assets, as set out in their cyber incident response and recovery plans. The team considered the following areas: (1) enterprise structuring of cyber security policies; (2) deployment of personnel resources, including defining roles and responsibilities; and (3) facilities and tools for response. The joint staff review team generally found the participants' plans and processes for incident response and asset recovery to be thorough. As described below, some larger participants responsible for multiple registered entities are moving toward an enterprise-wide cyber security approach, and implementation of their incident response and recovery plans is supported by full-time dedicated personnel resources. The joint staff review team recommends that cyber security incident response and recovery plans clearly identify who is responsible for asset response and recovery, specifically designating accountability at the cyber asset level (e.g., EMS servers, RTU concentrators, network routers, etc.), and recommends that measures be taken (including considering changes to the Reliability Standards) to address this issue. Although the joint staff review team recognizes that the Reliability Standards addressing resources, processes, and tools for cyber incident response and recovery will have improved clarity once the approved changes in CIP Version 5 become effective, consideration should be given as to whether the Standards as revised address all of the team's concerns in this respect. [61]

[61] *See NERC CIP Standards, version 3*, available at http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=

2. Review of Participants' Response and Recovery Plans

a) Enterprise Structuring of Cyber Security Policies

The joint staff review team found that the size of the participant organization influences the enterprise's structuring and approach to cyber security event response and asset recovery. Participants indicated that the larger the organization, the more likely that an enterprise-wide, top down approach is employed. Some of the largest participants use an enterprise-wide security policy to align all internal entities to the security and business goals of the overall organization, and are moving toward an overarching enterprise security plan.[62] In one example, a participant's plan calls for each business unit within the organization to apply the same cyber security incident handling procedures. For these participants, the enterprise-level policies require the operating companies and business units responsible for critical functions to develop and maintain a security incident response and recovery plan.

Although some smaller participants have business functions governed by enterprise security policies, they generally have more autonomous plans with security-related processes owned by an assigned team in each department or business unit. For these smaller organizations, enterprise-level involvement generally takes the form of review and approval of documentation related to the cyber incident response and cyber asset recovery plans and processes.

b) Personnel Resources, Roles, and Responsibilities

Participants indicated that their resource needs for cyber security have grown significantly in the last five years, and that they expect this growth to continue. All of the participants have full-time personnel dedicated to some aspect of cyber security and response, as defined in their cyber response and recovery plans.

United States. The Commission approved modifications to the currently-effective CIP Standards, referred to as the "CIP Version 5" standards. *See Version 5 Critical Infrastructure Protection Reliability Standards*, (Order No. 791), 145 FERC ¶ 61,160 2013).

[62] Internal entities could be wholly-owned affiliates, operating companies, member entities, different NERC-registered functional entities, etc.

Most participants maintain a cyber security response team responsible for the analysis and immediate response to cyber incidents, a cyber security response manager responsible for team governance, and a recovery plan owner responsible for document changes. These individuals are generally not the same personnel responsible for asset recovery. The classification and severity of a given event appear to dictate who is required to be involved in a participant's response. Large catastrophic events like a hurricane, which may result in the loss of critical cyber assets as well as physical equipment, may require most of the response groups mentioned, whereas finding a misplaced or unidentified USB device may require a single team response. The participants' plans varied in the level of detail in defining the personnel that need to be deployed for a given event type, and the particular approach taken. In defining cyber security plan roles and responsibilities, the level of detail of the response plans was shaped by several factors, including geography, size and structure of the organization and holdings, IT and network department size and structure, and vendor support required.

Regardless of the size of the organization, all participants assign roles to a plethora of individuals and groups in their established response and recovery plans, including: corporate IT help desk, telecommunications group, dedicated security teams, dedicated forensic teams, IT and technical managers, local law enforcement, support vendors, and other third parties. The joint staff review team found that a few of the review participants have a dedicated team for cyber security event response and asset recovery that works hand in hand with reliability standard compliance teams. However, from review of participants' plans and discussions with participants, the accountability of these individuals and groups was not always clear. Such a lack of clarity as to accountability could, during implementation, introduce confusion and result in reduced efficiency and effectiveness of recovery.

c) Processes and Tools for Response and Recovery

Processes Used for Event Assessment. All participants' plans characterize and classify the types or severity of events that would trigger the execution of a plan, but only some participants attempt to categorize the severity of all known potential threat events. Most of the participants' plans group events into an impact level of one to five, with the impact level dictating the response. To get an accurate assessment of the impact level, all events require response personnel and tools to perform the initial threat analysis. Whether complex or simple, all participants have an escalation process and response tools that require proper use, communication, and availability.

Facilities and Tools for Response. All of the review participants maintain redundant primary critical EMS/SCADA systems with a replicated backup system capable of assuming all functions in a short failover time. All participants have some degree of device redundancy on the primary system, allowing for high availability and quick recovery from a minor event. In addition to the primary and backup systems, all participants maintain some form of testing or development EMS/SCADA system that

mimics the primary system, and in an emergency situation can potentially be used as a spare.

While specific EMS/SCADA installations vary, most participants promote the use of secondary systems for recovery before resorting to data media backups. In fact, some participants do not use tape or other removable media for data backups at all, but instead rely on redundancy and hard-wired drive backups for data recovery. The participants that do use a robust tape data backup system use them for emergencies only. For data retention and restoration, the participants' plans identify approaches, hardware, and responsible personnel, with storage area networks and mirrored disk arrays the most popular approach to data restoration. Most participants do not keep a large inventory of replacement hardware, but rely on a third party for replacement of hardware that has failed.

3. Related Standards Assessment

Currently-effective Reliability Standards CIP-008-3 and CIP-009-3 include specific requirements to ensure that entities maintain planned resources for cyber security incident response and recovery of critical cyber assets. The relevant requirements for each standard are as follows:

CIP-008-3:

R1. Cyber Security Incident Response Plan – The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1 Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2 Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

CIP-009-3:

R1. Recovery Plans – The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1 Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

…

R4. Backup and Restore – The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

The joint staff review team found that Reliability Standard CIP-008-3 Requirements R1, R1.1-R1.2, and CIP-009-3 Requirements R1, R1.1, R1.2, and R4 are sufficiently detailed, enabling participants to effectively identify and maintain planned resources, processes and tools for response and recovery in their plans. However, the above requirements are not clear on accountability for assigned roles and responsibilities for response and recovery of critical cyber assets. This accountability is especially important for interconnected cyber systems which may involve several business units within an organization (e.g., accountability for recovering EMS servers, RTU concentrators, network routers, etc.). Lack of clarity about the accountability of assigned personnel could result in confusion and reduced efficiency of recovery during emergencies. [63]

Also, the joint staff review team found that an important element of security monitoring is to require *identification* of events as possible cyber security incidents, a task which has been more directly addressed in the CIP Version 5 Reliability Standards. [64] With that modification, the team otherwise found the requirements listed above to be clear and effective in promoting necessary planning on the resources, processes and tools to be used for cyber incident response and critical cyber asset recovery.

---

[63] The new CIP version 5 standards may address these concerns to some extent, but may not cover all potential areas of concern. *See* CIP-008-5 Requirement R1, part 1.3, and CIP-009-5 Requirement R1, part 1.2.

[64] CIP-008-5 Requirement R1 Part 1.1 requires applicable entities, for their High Impact BES Cyber Systems and Medium Impact BES Cyber Systems, to include one or more processes to identify, classify, and respond to Cyber Security Incidents. Mandatory compliance with the CIP Version 5 Standards will take effect in April 2016 for High and Medium Impact BES Cyber Systems, superseding the currently-effective Version 3 Standards.

4. Recommendations

Response and recovery plan ownership. The joint staff review team recommends that cyber security incident response plans and recovery plans for critical cyber assets specifically designate accountability at the cyber asset level (e.g., EMS servers, RTU concentrators, network routers, etc.). The team recommends that measures be taken (including considering changes to the Reliability Standards) to address this.

B. External Roles, Interrelationships, and Coordination

1. Summary

The joint staff review team examined the external roles, relationships and coordination required by or needed to implement the participants' cyber response and recovery plans. The team considered the following areas: (1) vendors, third-party support, and external dependencies; and (2) communications and relationships with federal and state law enforcement, task forces, and emergency management offices. The joint staff review team found that the participants have well-developed cyber security incident response plans that include communication plans and otherwise define roles and responsibilities with respect to third parties. The participants also have strong working relationships with local offices of the Federal Bureau of Investigations (FBI), Department of Homeland Security (DHS), and other law enforcement agencies for cyber security and emergency response. The joint staff review team did not identify any issues related to these areas, and found the relevant requirements in the Reliability Standard to be clear and effective in addressing these elements of a cyber incident response or critical cyber asset recovery plan.

2. Review of Participants' Response and Recovery Plans

Technical Support and Hardware. Although participants stress autonomy, all use third parties to varying degrees in support of their cyber security efforts, including technical support. All of the review participants maintain contractual and working relationships with system vendors for EMS and SCADA system technical support and hardware replacement. Participants also rely on EMS and SCADA vendors for security patch updates and assessments for those systems. Additionally, participants rely heavily on Windows and Linux operating system vendors for speedy security patch releases and fixes.

About half of the participants maintain some hardware inventory for critical devices, while the others rely on a third party or device redundancy for recovery. [65] Some participants use redundant dedicated telecommunication lines from vendors for high availability.

Cyber Security Monitoring. The participants primarily contract with third parties for penetration testing and security log analysis and alerting. Third parties responsible for security log reviews and event alerting report back to the participants' incident response teams or other responsible personnel identified in the cyber security response plan. Several participants use third parties in their review of policies, procedures, and restoration/recovery plans, with many reviews being a part of compliance with Reliability Standards.

Cyber Security Event Awareness. All of the review participants rely heavily on the Industrial Control Systems Cyber Emergency Response Team as the primary source for cyber security awareness, but they also rely on the Electric Information Sharing and Analysis Center (Electricity ISAC or E-ISAC), [66] vendors, and other outside sources.

External, Federal, and State Relationships. All participants, regardless of size, consider having working security and functional relationships with law enforcement and other outside entities to be important to their cyber security plans. All participants maintain relationships with relevant federal and state law enforcement entities and task forces, with many having dedicated liaisons to foster two way communication and awareness with these and other groups. Participants specifically mentioned having strong relationships with local offices of the FBI, DHS, and other law enforcement agencies. While all participants must have FBI and law enforcement contacts for events that must be reported on Department of Energy Form OE-417, [67] some participants explicitly

---

[65] The participants that do not maintain an inventory have system redundancy as a compensating measure. Apart from EMS and SCADA redundancy, the participants that maintain spare inventory appear to concentrate on network devices (e.g., firewalls, switches, etc.) and storage devices.

[66] The Electricity ISAC was previously named the Electric Sector Information Sharing and Analysis Center, or ES-ISAC, and the relevant CIP Reliability Standards still reference that name and acronym.

[67] The Department of Energy has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. See http://www.oe.netl.doe.gov/docs/OE-417_Instr-complete120508.pdf .

incorporate these law enforcement agency contacts in their emergency plans and procedures. These agency contacts may also participate in simulated drills and exercises of participants' emergency communication plans.

3. Related Standards Assessment

Currently-effective Reliability Standards CIP-008-3 and CIP-009-3 include specific requirements to ensure that the roles and relationships for cyber security incident response and critical cyber asset recovery are properly defined in the response plan, including any external roles and responsibilities and communication. The applicable requirements for each standard are as follows:

CIP-008-3:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following: . . .

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

CIP-009-3:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following: . . .

R1.2. Define the roles and responsibilities of responders.

The joint staff review team found that the participants have well-developed cyber security incident response plans that include communication plans and otherwise define roles and responsibilities with respect to third parties. Participants also have strong working relationships with local offices of the FBI, DHS, and other law enforcement agencies for cyber security and emergency response. For these reasons, the joint staff review team did not identify any clarity or efficacy issues related to relevant requirements in Reliability Standards CIP-008-3 and CIP-009-3.

C. Monitoring for and Detection of Cyber Incidents and Triggers for Incident Response

1. Summary

The joint staff team examined participants' monitoring for and detection of incidents, and triggers for incident response. The team considered the following areas: (1) monitoring methods and tools to detect anomalies and problems; (2) advances in programs, tools, and expertise for monitoring and detection; and (3) triggers requiring a response to a cyber incident. The joint staff review team found that the incident response plans for monitoring and detection of cyber security incidents vary across the range of participants, with the best of the reviewed plans having comprehensive escalation procedures, containing steps for further implementation based upon the complexity and/or depth and breadth of the threat or vulnerability, i.e. that 'escalate' when the threat or vulnerability risk increases, and make use of advanced tools, support, and expertise. Other reviewed plans lack well-defined characterization, assessment, and escalation of events. Therefore, the joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to address the use of specialized technical expertise, advanced tools, and levels of security expertise, to improve event monitoring and response. The team also recommends that measures be taken (including considering changes to the Reliability Standards) to require details around the types of events that should trigger a response and what type should be reported.

2. Review of Response and Recovery Plans

a) Monitoring Methods and Tools to Detect Problems

In comparing participants' cyber incident monitoring methods as set out in their respective plans, the joint staff review team found two major areas of system monitoring pertaining to bulk power system reliability: (1) monitoring cyber system performance, and (2) authorized use of critical assets, critical cyber assets, and their supporting cyber systems. The participants apply controls in various ways to help determine whether critical systems have unwanted or unauthorized activity, and use that information to determine how and when to respond.

Participants' system monitoring consists of automated tools used to monitor network traffic, and can be system-based or host device-based. Participants indicated that the monitoring systems can generate a large quantity of data, and that effective data management tools are therefore important for effective monitoring. Participants indicated that a new threat identified for monitoring can have significant ramifications on operations and often requires timely and appropriate response to the threat. Cyber threat events chosen for monitoring can cover a wide range of activities, such as: (1) new or existing services on host devices suddenly being utilized, (2) unusual login times and unsuccessful attempts, (3) abnormal traffic on a network, (4) changes to a file's integrity

and attributes, and (5) escalation of administration rights and suspect network behavior (i.e., traffic/protocols outside the norm).[68] Most participants' response plans have established thresholds for a suspected cyber threat event that may trigger a pre-determined response.

One threshold indicator used by participants automatically assesses large quantities of data, and sends notifications to an Incident Response Team member(s) once a pre-determined trigger is met. The alert notification may prompt additional intervention using manual processes, making it necessary for technicians to manually review the data to determine whether the detected activity should be considered suspicious, warranting further response and threat level escalation, or considered a false positive indication.

Every review participant stressed the importance of having round-the-clock coverage to receive and respond to alert notifications. Some participants have established a dedicated security operations center[69] as an in-house cyber incident and threat assessment center. Security operations center technicians perform the initial analysis of any alert and/or detected suspicious activity. Participants that do not use a security operations center model rely on their subject matter experts or use third-party vendors to process alert notifications. In some cases, participants use a hybrid approach: employees perform the task during business hours and a vendor or network operations center provides support for the balance of the time.

Most information used to perform this analysis comes from an intrusion detection system, but intrusion prevention systems are becoming widely implemented within participants' organizations as well. Organizations may also deploy application whitelisting on user devices, permitting only specified activities, interactive access, and specific processes and programs to run.[70] Another emerging trend is the use of behavioral profiles for each

---

[68] From discussions with the participants and their use of different naming conventions, the joint staff review team chose to use the phrase "cyber threat events" to refer to participant-monitored cyber events that are not yet determined to be cyber security incidents or a cyber threat that did not rise to the level of an entity-declared Cyber Security Incident as defined in the CIP standards (e.g., scanning an IT system for a newly discovered threat described by ICS-CERT).

[69] "Security operations center" is a generic name used in this report to describe a dedicated security monitoring operation.

[70] An application whitelist is a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a system according to a well-defined baseline. *See* National Institute of Standards and Technology, U.S.

authorized user, so that when a known user's activity deviates from typical behavior, that activity is flagged for further analysis.

b) Implementing Advanced Cyber and Physical Threat Programs and Tools

Participants use a number of third-party vendor products in their cyber security and threat detection programs, procedures, and processes. As participants strive to keep abreast of new and evolving cyber and physical threats, they are partnering with third-party cyber security specialist vendors. Several participants have joined cyber security awareness groups sponsored by governmental authorities, and are working with universities that have advanced cyber security programs. Also, participants' cyber security professionals are coming together to form groups or charters with professionals in similar business or operational models, in an effort to keep current with threats specific to their industry. Some participants have hired cyber security professionals with advanced skills and capabilities to develop advanced in-house cyber security operations centers, and plan to partner or extend their services to other entities outside of their NERC functional registration and footprint. The joint staff review team found that participants' cyber security threat detection teams are staffed with personnel from specialized operational functions such as IT and networking groups that together form a larger cyber security incident command.[71]

Participants acknowledged that developing thorough internal control processes is key for mitigating certain types of slow advanced persistent threats, in which a bad actor or actors can penetrate a system and move across networks while elevating existing accounts and access privileges.[72] Development of internal control processes may require

---

Department of Commerce, *NIST Special Publication 800-167 (Draft) Guide to Application Whitelisting* (August 2014).

[71] The cyber security group may draw from a typical network operations center, IT support group, 24/7 Help Desk, and EMS/SCADA support. Such a group will use system-specific tools such as intrusion detection systems, hardware monitoring, antivirus, network inspection tools, and security information and event management to inspect network traffic, log files, and logon access.

[72] An advanced persistent threat attacks information assets of national security or strategic economic importance through either cyberespionage or cyber-sabotage. These attacks use technology that minimizes their visibility to computer network and individual

actions such as trusted authorization tickets segmenting business groups. Some participants require additional sponsorships for administrative changes to existing or newly-created user authorization account access, and for escalation of privileges and rights. The use of additional sponsorships or similar processes could help prevent an administrative level insider threat or an escalation of rights attack from an advanced persistent threat. Participants' response plans apply a defense-in-depth posture that includes network detection tools and capabilities, such as host-based intrusion detection systems, antivirus, physical access control systems for physical intrusion threats, EMS/SCADA alarms, firewalls, peripheral system alarms and internal notifications to the 24/7 cyber security monitoring centers described above. Some participants have established a centralized logging system for inspecting many of their system software, login access and physical access controls systems. Participants indicated that specialized software tools and systems can aid in inspecting log files and identifying anomalies for large amounts of data, but that the process of human inspection and intervention is still necessary to determine whether a flagged suspicious item is an actual threat or, for example, an employee who exceeded his or her password attempt limit. [73]

c) Triggers for Responding

All of the review participants have dedicated personnel focused on monitoring systems and devices from a cyber security perspective, and it is common for a participant's IT Help Desk to be the initial point of contact for this monitoring. Users who may detect an anomaly within their environment can report issues through established protocols. Participants' monitoring processes include assigning the reported issues a priority level commensurate with their importance, so business systems may not have the same response expectations as a system critical to operational reliability. Regardless of the

---

computer intrusion detection systems. Advanced persistent threats are directed against specific industrial, economic, or governmental targets to acquire or to destroy knowledge of international military and economic importance. Once an advanced persistent threat has entered its target, the attack can last for months or years; that is, it is a "persistent" threat. *See Encyclopædia Britannica Online*, s.v. "advanced persistent threat (APT)", accessed September 01, 2015, http://www.britannica.com/topic/advanced-persistent-threat.

[73] The team noted that some of the participants, through third party provisions, use advanced monitoring tools which automatically collect and compare information to perform wider-area monitoring for detection of cyber security events.

notification method (Help Desk or automated alert), once a possible incident is determined to warrant further analysis, participants' processes involve initiating the appropriate technical support to evaluate the factors and information pertaining to the alarm/report. Recently, some participants implemented specialized 24/7 incident response teams and a hotline for reporting any suspicious activity or anomaly identified in log files, alarms, communication protocols and changes in system performance. The incident response team may be staffed by in-house operational personnel with IT, network and cyber and physical security experience and backgrounds. Once notified, the incident response team can assess an issue and contact support personnel with the necessary specialized expertise in networks, firewalls, EMS/SCADA systems, cyber threats, and communication systems.

Some participants use a matrix table to evaluate, characterize, and determine the type of cyber threat events occurring on their system or being reported in cyber security alerts, notifications, and advisories. The initial assessment determines if a more thorough review is required. The relevant details are routed to the designated response personnel responsible for business units and operational functions that may be impacted. This routing includes any 24/7 third-party vendor support for cyber security detection and prevention systems employed. For some participants, this more thorough review is fulfilled by a cyber security incident response team sometimes referred to as a cyber security operation center. Some participants are partnering with various specialized cyber security vendors, intrusion detection systems, intrusion prevention systems, and services for more in-depth cyber threat event detection and analysis to identify and help classify events.

Participants' response plans commonly include comparing an event with the matrix criteria, table spreadsheet, or other method used to determine the initial risk assessment and impact, and initial cyber threat event level. Participants apply these methods to obtain an accurate initial cyber threat determination level, which will then initiate the response required for that cyber threat level. The incident response team's response to the event may reveal whether a more serious threat criteria level is present and trigger a greater threat cyber incident level. This increase in incident level may also trigger a different response and additional evaluations, mitigating actions, and notifications. Several participants noted that, while initial threat event classifications are critically important, the triggers and threshold criteria for escalating and de-escalating the level of a threat event are equally important and need to be well understood.

3. Related Standards Assessment

Currently-effective Reliability Standard CIP-008-3 and other standards include specific requirements regarding the monitoring of cyber security events and events or actions responsible for triggering a response.[74] For CIP-008-3, these include:

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1 Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2 Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

The joint staff review team found that the incident response plans and monitoring programs vary across the range of participants. Several more robust plans have comprehensive escalation procedures, use advanced tools and expertise, and maintain third-party support for monitoring and detecting cyber security incidents. Other participants have less robust plans, which are not as well defined regarding the

[74] Reliability Standard CIP-007-3 Requirement R6 requires responsible entities to ensure that all Cyber Assets within the electronic security perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security, and requires maintaining logs of system events to support incident response, as required in CIP-008-3.

Reliability Standard CIP-005-3, Requirement R1.5 requires Cyber Assets used in the access control and/or monitoring of a responsible entity's Electronic Security Perimeter(s) to be afforded the protective measures specified in Standard CIP-008-3. This sub-requirement pulls network communication devices responsible for protecting the electronic security perimeter into the security monitoring requirements of CIP-007 Requirement R6.

The team did not address CIP-006-3 Requirement R2.2, which refers to CIP-008-3, because the sub-requirement pertains to physical security perimeters and mechanisms.

characterization, assessment, and escalation of events, due to a lack of expertise, advanced tools, and third-party support.[75] Use of advanced tools, expertise, and third-party support is not required by CIP-008-3 or by any other relevant Version 3 CIP Reliability Standard. Also, as described above in the section "Planned Resources, Processes, and Tools for Response and Recovery," the joint staff review team observed participants with processes that also include *identifying* events as possible cyber security incidents. CIP-008-3, R1.1 requires procedures to characterize and classify events as reportable cyber security incidents, but does not require identification of the types of possible triggering events as such.

As noted above, this important element is addressed more directly in the CIP Version 5 Standards, which requires each responsible entity to have processes to identify Cyber Security Incidents.[76] Also as described above, in striving to keep abreast of and respond to new and evolving cyber and physical threats, participants recognize the importance of utilizing cyber security technical expertise and advanced tools. The team recognizes that

---

[75] Recognizing the benefits of the use of advanced resources and expertise, some participants employ extensive monitoring programs, while a few rely heavily on complex escalation procedures, advanced tools and third-party support. For the latter participants, the lack of a more streamlined process may introduce room for error.

[76] Reliability Standard CIP-008-5, Requirement R1, Table R1 Part 1.1 requires each responsible entity to have a process(es) to identify Cyber Security Incidents.

The Nuclear Regulatory Commission (NRC) recently adopted a cyber security event reporting rule which specifies, for nuclear licensees and licensee applicants, the kinds of cyber security events that must be reported and the time frame for reporting (from one hour to twenty-four hours depending on the type of event). For example, the NRC requires licensees to notify the NRC within one hour after discovery of a cyber attack that adversely impacted safety-related or important-to-safety functions, security functions, or emergency preparedness functions (including offsite communications), or that compromised support systems and equipment resulting in adverse impacts to safety, security, or emergency preparedness functions within the scope of 10 CFR § 73.54 (Protection of Digital Computer and Communication Systems and Networks). The rule also requires licensees to notify the NRC within four hours of a cyber attack that could have caused an adverse impact to the above, and defines the kinds of events that require notification within eight hours or twenty-four hours. *See Cyber Security Event Notifications*, NRC-2014-0036, 80 Fed. Reg. 67264-01 (Nov. 2, 2015).

CIP Version 5 does not specifically require the use of these; however, through entities' implementation of CIP Version 5, additional insight may be gained to aid in considering future changes to the Reliability Standards to address these important cyber security areas.

4. Recommendations

Use of technical expertise and advanced tools. The joint staff review team has concluded that cyber event monitoring and response would be greatly improved by expanding the use of cyber security technical expertise and advanced technical tools, and recommends that measures be taken (including considering changes to the Reliability Standards) to address the use of these tools to improve cyber event monitoring and response. In considering such measures, it may be appropriate to allow for some experience with CIP versions 5 and 6. In addition, the team recommends that such measures clarify that these advanced tools and resources should be employed in a manner that does not negate the benefits by making the cyber security event monitoring process more cumbersome or unnecessarily burdensome.

Require details on types of cyber security events that should trigger resp reporting. The joint staff review team also recommends that measures be taken (including considering changes to the Reliability Standards) that address the need for cyber security incident response plans to include details around the types of cyber events that should trigger a response (e.g., EMS or SCADA outage, communications network outage, etc.), and what types should be reported. While the team recognizes that CIP version 5 will require responsible entities to have processes to identify cyber security incidents, consideration should be given as to whether any additional clarification or improvements are needed once some experience is gained with CIP version 5.

D. Initial Event Response Actions

1. Summary

The goal of initial cyber event response analysis is to assess whether a given cyber alert or activity warrants further action. Initial event response analysis is a critical step in the response process. In its review of participants' initial event response actions, the joint staff review team examined: (1) triage, (2) bulk power system impact determination, (3) escalation methods and protocols, and (4) event data gathering and containment.

As described below, the joint staff review team did not identify any clarity or efficacy issues with the pertinent Reliability Standards with respect to initial event response actions. The review team recommends that entities consider use of hybrid systems that use a combination of both automation and human analysis as part of initial event analyses.

2. Review of Participants' Response Plans

a) Triage

Most participants use multiple levels or tiers of organizational response for cyber security events, often using a "triage" approach to determine whether further action is warranted and by whom. The triage approach generally includes implementing policies and procedures that address event classification, escalation, responsibilities for response, and reporting obligations.

Some participants have 24/7 dedicated cyber response teams (e.g., incident response teams) with expertise in identifying and tracking cyber threats across the enterprise, while others partner with an existing cyber security service or third-party vendor service. Most participants maintain response teams comprised of employees pulled from business units such as IT, networks, and EMS SCADA to form their incident response team as needed. The incident response team will initially analyze a cyber threat event to determine the degree of response required to address it. For example, if a recently discovered vulnerability identified by the United States Computer Emergency Readiness Team for a particular device (firmware, software version, and release) exists on a participant's system(s), that participant will require a level of response and triage from the incident response team that mitigates the risk and exposure to the entity and the bulk power system.

b) Bulk Power System Impact Determination

The initial steps of an event assessment are focused on the critical systems and locations affected by (or affecting) an event, and on determining the necessary expertise required to assist in mapping out the next steps. All of the review participants employ this approach for their initial response to potential events.

The participants each conduct an in-depth review to assess the potential for a given cyber threat or anomaly to impact the bulk-power system, which includes an analysis of anomalies detected through log inspections and evaluation. This review is typically performed through automation, but the majority of the review participants employ a hybrid system, using a combination of both automation and human analysis. Systems and tools used for this analysis include intrusion detection systems, intrusion prevention systems, inspecting system logs, networking traffic analyses, and other analytical tools. The analysis includes a review of available patches for systems and devices and, if a specific issue or vulnerability is being considered, specialized tools or processes may be used. The joint staff review team believes this hybrid approach to event assessment enhances the industry's ability to respond to cyber security incidents.

c) Escalation Protocols and Methods

All participants rely on a tiered approach to escalation protocols. In a tiered approach to incident response, the event is handled at the lowest tier possible so that the entity does not waste resources when an event does not warrant the full incident response team. One participant uses a four-tiered approach, in which attempts are made to contain and mitigate the event within each tier before moving on to the next higher tier. Various tools for mitigation, detection, monitoring, and forensics are used at each tier with more sophisticated tools used in the higher tiers.

d) Event Data Gathering and Containment

Some of the participants use an enterprise operations center[77] to help with their event analysis and containment of an event while others employ numerous processes and procedures within different departments or functional areas. As noted above, the designated response teams assess the potential impact on EMS or SCADA system availability and take steps to manage that impact.

To help limit the potential propagation of a given cyber threat and to allow for identification of threat sources, all participants use a number of internal security measures and practices. The majority of participants use full time employees where possible for positions that include some level of access to cyber systems. This practice is particularly important for sensitive positions as it limits the entity's exposure to outsider threats and the potential for further propagation of an event. Some of the participants will retain the records of an employee's access to critical cyber systems for up to one month following his or her departure. This record retention practice is mainly for documentation and maintaining a paper trail. Otherwise, supervisors update and revoke access privileges within five days of an employee's departure. One participant takes a different approach to monitoring systems and devices, monitoring every device that is on the network. This approach limits employee lists to a minimum and helps enable the detection of rogue devices that do not belong on the network.

3. Related Standards Assessment

While Reliability Standard CIP-008-3 does not dictate a particular form for initial event response and analysis, it does require applicable entities to have a plan that addresses

[77] An enterprise operations center is a group of dedicated employees that review and analyze network traffic data looking for anomalies and/or potential threats to the enterprise network.

"response actions" to cyber incidents, which necessarily includes some form of initial analysis and triage:

CIP-008-3:

R1 Cyber Security Incident Response Plan - The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

…

R1.2 Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

Though the requirements are broadly written and require little in the way of criteria defining an adequate cyber security incident response plan, the joint staff review team found that the participants' plans address, in detail, initial event response actions. All use a tiered approach for triage, and their plans include implementing policies and procedures that address event classification, escalation, responsibilities for response, and reporting obligations. The team's review of participants' plans did not reveal any concerns with the clarity and efficacy of the associated Reliability Standards for these areas, particularly given the approved changes to the standards that will become effective as part of the CIP Version 5 Standards. [78]

4. Observed Practices for Consideration

Some participants' plans include a hybrid system for determining bulk power system impact or threat from a cyber incident. The joint staff review team considers hybrid systems that use a combination of both automation and human analysis to be a beneficial practice for consideration by the industry.

[78] Reliability Standard CIP-008-5 includes several new provisions, including: Requirement R1.1, which requires one or more processes to identify, classify, and respond to Cyber Security Incidents; Requirement R1.3, which addresses the roles and responsibilities of Cyber Security Incident response groups or individuals, and Requirement R1.4, which addresses incident handling procedures for Cyber Security Incidents.

E. Recovery Planning

1. Summary

It is crucial that entities have effective recovery plans for critical cyber assets in response to events. The joint staff review team accordingly reviewed the participants' recovery plans and associated testing practices, by examining the stages and processes of participants' recovery plans.

The joint staff review team found that participants' recovery plans for critical cyber assets address the stages and processes of recovery planning included in Reliability Standard CIP-009-3. Participants' plans for recovery from events have well-established strategies for staffing, logistics, emergency facilities, and communications methods, described in detail below. However, the team found assumptions in some participants' recovery plans that could risk a timely recovery. The joint team recommends that measures be taken (including considering revisions to the Reliability Standards) to ensure that recovery plans do not include or implicitly rely on any major inventory assumptions (e.g., assumptions of hardware being available without measures to ensure availability) for critical cyber assets that could significantly affect prompt recovery of critical cyber assets. These measures would mitigate the potential risk of delayed recovery resulting from such assumptions.

2. Review of Participants' Recovery Plans

Participants' recovery plan scenarios are categorized by the severity of the actual event or an anticipated event such as severe weather. Participants' plans for actual and anticipated events have well-established strategies for staffing, logistics, and emergency facilities. Critical to their restoration and recovery efforts are reliable communication protocols and backup communication systems throughout their organizations, departments, business units, groups and personnel identified in the recovery plan. Some of the participants have incorporated related lessons learned into their response and recovery plans, with provisions for an extended loss of communications due to extended power outages, loss of telecom services (landlines, Voice Over Internet Protocol, and mobile), corporate e-mail services, etc.

All participants' response and recovery plans identify the key contact personnel (and backups) by name and department, and owners of the plans. The participants' recovery plans include the plan's objectives and goals at the highest level, and become more granular and specific by the classification of assets or primary business functions. As the recovery plans become more granular and specific by department and function, the plan specifics are to be implemented by designated top level department personnel. Changes to specific recovery plans for most participants require approvals from personnel responsible for that asset, who are generally department heads, and final approvals from the personnel responsible for the entire recovery plan.

Some participants' cyber asset recovery plans enlist corporate IT support and network operations center support because these groups often operate around-the-clock and overlap with many departments and systems, including critical assets, critical cyber assets, and non-critical cyber assets. Specialized groups and owners of a critical asset or critical cyber assets may have sole jurisdiction and ownership of their physical and cyber assets and will determine the level of response required and recovery procedures in their recovery plan.

Under the participants' recovery plans, the first personnel to respond to a given problem or event involving a critical cyber asset will start with troubleshooting their operational systems, business systems and supporting systems. As the cause of the problem becomes more evident, the group enlists other groups and individuals as needed and as identified in their response and recovery plan, including IT support, network support, and vendor support, for both software systems and hardware systems.

As better information becomes available, the scope of the actual and potential threat is assessed and initial response and recovery plans are activated. Participants indicated that it may require days, weeks, or longer to determine the actual root cause of a given cyber event and its impact on various assets types and systems. Specific hardware and software components and specific business functions affected may trigger escalation to a greater severity threat categorization or de-escalate into a lesser response category, as the affected resources may (or may not) be critical assets, critical cyber assets, or non-critical cyber assets that are otherwise important for operations and business functions. There may also be interdependence on vendor response and assistance for critical cyber asset EMS and network systems and supporting business systems.

Participants' plans include procedures for varying levels of loss or degradation of critical assets and critical cyber assets and supporting non-critical cyber asset systems, software, and hardware components. The recovery plans detail a number of response levels for potential events ranging from total physical loss of a critical asset facility, operational loss of a critical cyber asset facility, EMS control center and SCADA loss or degradation, loss of business processes, to the loss of server or network components, including switches, routers, firewalls, and remote terminal units.

The participants' plans vary regarding the back-up computer hardware or other equipment inventory assumptions used for their asset recovery methods. Some participants rely on vendors in part for recovery of their critical cyber assets, but do not necessarily take into account that a particular vendor may need to supply equipment to multiple entities during a large scale event, or otherwise take into account interdependent or common-mode failure scenarios.

3. Related Standards Assessment

Reliability Standard CIP-009-3 requires applicable entities to have processes and procedures in place to recover, backup, and restore critical cyber assets, as follows:

CIP-009-3:

R1. Recovery Plans – The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

…

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

As noted above, the participants' plans vary regarding the back-up computer hardware or other equipment inventory assumptions used for their asset recovery methods, and the above Reliability Standard requirements allow significant variance in how an entity can recover from a cyber event. For example, some participants rely on vendors, in part, for recovery of their critical cyber assets. In a large scale event, a particular vendor may need to supply equipment to multiple entities. The assumptions may not take into account interdependent or common-mode failure scenarios, which can create the need for multiple entities to recover multiple critical cyber assets from the same vendor(s). Other assumptions may compound this risk, including assumptions regarding availability of spare components from backup facilities or offices that may not be available when needed during the event, and assumptions regarding telecommunication services (cellular and landlines) and e-mail services, which may not be available when needed. Reliance on the assumption that vendors will have the equipment available without some contractual or other guarantee, or otherwise maintaining on-site inventory of vital hardware, could result in a significant delay in asset recovery.

As industry moves toward a more virtual environment, having an effective action plan to restore critical cyber assets is essential. From its review of the participants' critical cyber asset recovery plans, the joint staff review team found that the Reliability Standards need

to be clarified in order to effectively support reliability by requiring entities to eliminate any major assumptions incorporated in their recovery plans and procedures which could significantly affect prompt recovery of critical cyber assets. The joint staff review team realizes that it is not possible to eliminate all equipment inventory or availability assumptions, but reliance upon vendors for inventory management may impose significant risk unless availability and timely delivery of replacement hardware is written into contracts. Other such assumptions should also be avoided in order to improve the entity's response to events.

4. Recommendations

Recovery plan inventory assumptions risk. The joint staff review team recommends that measures be taken (including considering changes to the Reliability Standards) to eliminate, to the extent possible, "inventory assumptions" in cyber asset recovery plans that could significantly affect prompt recovery of critical cyber assets. For example, entities may assume that hardware from external sources or other third-party vendor support needed for recovery of critical cyber assets will be available, without necessarily having measures to ensure availability. Likewise, entities may not consider interdependent or common-mode failure scenarios, which can create the need to recover multiple critical cyber assets concurrently from the same vendors.

F. Review and Verification of Incident Response and Recovery Plan

1. Summary

The joint staff review team examined how participants verify the viability of their cyber incident response and critical cyber asset recovery plans, including their periodic reviews of the plans and testing of plans and associated facilities and resources.

As described below, the joint staff review team found that the participants' response and recovery plans address in detail confirmation of the viability of the plans by testing the plan facilities and resources. The joint staff review team nevertheless concludes, for reasons discussed below, that all applicable entities should consider having an independent third party review their cyber incident response and critical cyber asset recovery plans to ensure they are thorough and reliable.

The joint staff review team also observed certain practices that appear to enhance the participants' cyber incident response and recovery planning and testing, and recommends that applicable industry entities consider implementing these approaches in their own recovery plans. Observations by the joint staff review team are detailed below.

2. Review of Participants' Response and Recovery Plans

a) Periodic Reviews of Response and Recovery Plans

Most participants review their cyber security incident response and critical cyber asset recovery plans in-house, with few participants undertaking independent reviews. Of the few participants that use third-party reviewers, only two have multiple independent companies review their plans. One participant, in addition to using independent reviewers, also performs a bi-annual internal CIP sufficiency review to better ensure that it can handle potential cyber security incidents. Those participants who have independent reviews expressed that while these reviews may not in all cases be superior to an in-house review, an independent review of a recovery plan can provide an unbiased perspective and validation of the plan. In addition, these participants indicated that an independent review can provide added value and expertise, and incorporate industry best practices, particularly if the reviewer has the capability and experience of reviewing many industry-wide plans, information and data (i.e., can provide a more comprehensive perspective).

b) Testing of Response and Recovery Plans

The ways in which participants test their response and recovery plans are specific to each participant. Almost all participants use real world events that have either occurred to the participant or to other entities in setting up their testing or exercise scenarios. As described further below in the Drills and Training Exercises section, participants' incident response and recovery plan testing predominantly consists of tabletop paper drills.

The increasing sophistication of cyber security events is driving entities to scrutinize their recovery plans, and evaluate through testing and exercises whether existing recovery resources for critical cyber assets are adequate. Effective recovery plans consider and plan for both small and large impact scenarios.

c) Testing of Recovery Resources

Participants generally test their ability to recover critical cyber assets and associated recovery resources during their back-up control center drills. Some participants' tests are limited to staff traveling to the backup center and powering up the backup resources. Other participants conduct drills for a complete site loss of cyber assets, such as complete loss of a control center or forced site evacuation leading to the transfer of operations to an alternate control center, with some operating for an extended length of time (e.g., greater than 24 hours). Through discussions with participants, the joint staff review team found that exercises involving the actual transfer of control center operations to an alternate site for a period of time are more realistic tests of the functionality of recovery resources than a simple power up of backup control center operations. The drill or actual evacuation event can and often does reveal unknown issues or problems at the alternate site's

SCADA EMS system. Moreover, by running exercises from an alternate control center system for an extended length of time, entities can better evaluate support issues and needs at the alternate site, including the logistics of extended site transfers and the peripheral system needs for running operations at the alternate control center for extended periods of time.

In addition to high impact scenarios, participants often conduct recovery exercises of event scenarios of lesser impact, both in size and scope. These lesser impact scenarios are important, because from a risk perspective, such events are more likely to occur than large catastrophic events. Recovery exercises and scenarios may include a single system loss, network system interruptions, hardware server loss, or loss of a functional system component that can disrupt normal operations and critical business systems.

The joint staff review team found that some participants employ virtualization software to facilitate recovery. Virtualization software products and virtualization technologies can aid servers, workstations and other cyber assets in recovery from unrecoverable hardware disk crashes, corrupted software systems or components, and workstation terminals. In addition to tape backups, a few participants are also using a type of virtual backup referred to as a "golden image" for their critical servers and software components and for network devices like switches and routers.[79] A golden image can significantly reduce the restoration time required to build from a new hardware device. Device restoration is much faster from an imaged software and file system than restoration from files on disk or tape drives.

Discussions with the review participants revealed that conducting certain recovery tests on a live production system or the backup or alternate system is not advisable. This is due to the fact that additional risks may be introduced into the recovery system or facility (e.g., EMS server replacement) that could jeopardize the functionality of the production system or the backup system. For instance, unknown problems with the recovery device could propagate to other production system critical cyber assets (e.g., EMS/SCADA) and prevent the original device from being restored. To this end, participants have installed fully representative test systems for their CCAs and EMS SCADA control systems. Using such a test system, often referred to as a quality assurance system, an entity can

[79] In network virtualization, a "golden image" is an archetypal version of a cloned disk that can be used as a template for various kinds of virtual network hardware. The golden image is a master image from which copies can be used to provide a consistent process for creating a disk image. The use of golden images in cloud computing solutions can provide consistency for rebuilding hard drives for recovery or pushing out updates across various virtual machine desktops.

perform full functional testing and restoration and recovery exercises on a system identical to its production environment. In addition, the quality assurance system can also provide spare components in an emergency situation.

Participants expressed that they are continually improving and increasing the availability and redundancy of the EMS control center's systems for operations and business continuity. Advances in both computer EMS software systems and communications between primary control center and alternate control center (such as hot standby and heartbeat) are increasing operational availability and lessening system recovery times. [80] Advances in restoration techniques, virtualization software techniques, and disc imaging are decreasing hardware restoration times compared to restoration from disk and/or tape backup media.[81]

The joint staff review team observed that many participants have spare hardware servers available for testing the recovery of failed servers, switches and firewall components. Some participants have pre-configured hardware servers available as spares. Restoration from a virtualized image in recovery has reduced recovery times significantly compared to restoration from disk or tape drive. However, the actual recovery media entities use, whether virtualized image, disk or tape backup, depends on their particular systems, the amount of data being recovered, and the cost of the solution employed. Participants mentioned that, for emergency situations, having the option of using spare components from identical and redundant systems can shorten restoration and recovery time. EMS servers can be imaged from the alternate EMS system servers or a representative test system such as the quality assurance system.

---

[80] An EMS 'Hot Standby' is a primary EMS and a fully functionally redundant backup EMS system, configured in a constant state of readiness for a quick and seamless takeover if the currently configured primary EMS system's functionality deteriorates or becomes unavailable. In the 'heartbeat' communication process, the currently configured backup EMS continually monitors the health of the current primary EMS's critical processes and functionality. If the currently configured backup EMS (in hot-standby mode) detects a signal or flag that the health and functionality of the Primary EMS is lost or deteriorating, it will start the process of taking over as the primary EMS with complete SCADA functionality.

[81] A disk image is a copy of the entire contents of a storage device, such as a hard drive, DVD, or CD. The disk image represents the content exactly as it is on the original storage device, including both data and structure information. A disk image of a hard drive may be saved as a virtual hard disk.

3. Related Standards Assessment

Reliability Standard CIP-008-3 includes requirements pertaining to review and testing of incident response plans, and Reliability Standard CIP-009-3 includes a requirement for testing backup media essential to critical cyber asset recovery, as follows:

CIP-008-3:

R1. Cyber Security Incident Response Plan – The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

…

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-009-3:

R1. Recovery Plans – The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R5. Testing Backup Media – Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

Consistent with these requirements, the participants' plans address the need for periodic review and testing of cyber incident response and critical cyber asset recovery plans. However, while the Reliability Standards currently require annual review of plans and approval by a senior manager or delegate, they do not require plan review by an independent party. As noted above, the joint staff review team concluded from review of

the plans and discussion with the participants that independent review of policies, processes, and technical mechanisms included in cyber incident response and critical cyber asset recovery plans can provide an unbiased, more comprehensive perspective. This independent review approach is similar in purpose to other independent reviews required under the Reliability Standards, including reliability coordinator review of a transmission operator's restoration plan under Reliability Standard EOP-005-2. The joint staff review team notes that the projected entity resources needed for conducting an independent review are expected to be similar to those needed for an in-house review or an audit. The team also notes that many of the participants are already employing third-party reviews for compliance review, and that some use third parties for technical best practice reviews. Moreover, many of the participants have established close working relationships with third parties to help stay abreast of developments on cyber threats and prevention approaches, including information received from other electrical sector entities and local government agencies, which information is used as part of these participants' internal reviews.

Notably, under new Reliability Standard CIP-014-1 (Physical Security), applicable entities are required to have an unaffiliated third party verify their required risk assessments identifying critical transmission stations and substations, i.e., those that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Given that cyber environments are similarly unique, numerous and complex, and create a kaleidoscope of threat and vulnerabilities that will demand unique responses, the joint staff review team believes that the industry as a whole could benefit from independent review of responsible entities' cyber incident response and critical cyber asset recovery plans.

4. Recommendations

Independent review of cyber security response and recovery plans. The joint staff review team recommends that recovery plans for critical cyber assets and cyber security incident response plans be reviewed by an independent authority or third party for the purpose of supporting thoroughness and technical reliability, using a trusted or otherwise qualified third party to ensure a proper security review.

5. Observed Practices for Consideration

In evaluating participants' response and recovery planning reviews and testing, the joint staff review team observed the following practices and recommends consideration of these by other relevant entities:

- Some participants perform exercises or drills that involve the actual transfer of control center operations to an alternate site for a period of time, to test the functionality of the recovery resources. This practice provides a more realistic test of response and recovery readiness as compared to only powering up the backup

resources to test their functionality. The drill or actual evacuation event and verification of functionality of recovery resources can and often does reveal unknown issues or problems at the alternate site's SCADA EMS system.

- Some participants perform exercises or drills that require failover to their backup control centers for drills for more than just a few hours. This practice tests whether support systems and other support resources that are needed to run from the backup are readily available and remain available, and allows personnel to become familiar with running from the backup center instead of the primary center. Entities running exercises from their alternate control center system for an extended length of time can better assess support issues and needs, such as the logistics of extended site transfers and the peripheral systems needed for running operations at the alternate control center for extended periods of time.

- Some participants use a type of virtual backup referred to as a golden image for their critical servers and software components and for network devices like switches and routers. This practice can significantly reduce the restoration time required to rebuild and implement hardware that replaces affected hardware during the recovery process, versus utilization of disks or tape storage. Further, reliance upon identical assets used in support environments (e.g., off-line development system assets) to recover the EMS/SCADA production environment can have some drawbacks, due to less-frequent usage and/or software updates.

G. Drills and Training Exercises

1. Summary

The joint staff review team examined how participants' cyber incident response and critical cyber asset recovery plans address drills and training exercises. The team found that the participants' plans require periodic testing or exercising of the response and recovery plans, including testing of backup communications systems and other backup systems used in the plans, typically exercised in the form of tabletop exercises or actual drills. The joint staff review team found that participation in full operational exercises and other more complex simulations provides greater insight into the viability of a given cyber response and recovery plan, and appears to be necessary to develop robust recovery and response plans. Further, participants that have participated in regional tests/exercises which incorporated interdependencies have developed more robust recovery and restoration plans than those that only perform tabletop exercises. The joint staff review team recommends that entities consider, as a best practice, conducting full operational

exercises or other more complex simulations of their cyber incident response and critical cyber asset recovery plans, including testing for interdependencies and other vulnerabilities.[82]

2. Review of Participants' Response and Recovery Plans

a) Regional Cyber and Physical Recovery Exercises

One participant held a voluntary exercise simulating a focused cyber and physical attack on the functional entities in its footprint. Another participant engaged in an exercise that the Federal Emergency Management Agency (FEMA) performed in its region, focused more on severe natural disaster conditions (i.e., earthquake, mudslides, tornadoes, hurricanes, etc.), but which extended to recovery of critical cyber assets. This specific exercise was the first conducted by FEMA, but with the success of this exercise, the participant indicated that it is expected to become an annual exercise.

Another review participant enrolls in its reliability coordinator's restoration drill, which involves every entity within the reliability coordinator's footprint. The participant then performs its own large scale exercise, including hypothetical toxic fumes with evacuation of facilities and a complete loss of communications.

In addition, some of the larger participants have held a wide area testing scenario for their footprint, and have invited neighboring utilities to participate in these events. The joint staff review team observes that conducting wide area testing scenarios is a worthwhile practice that the industry should consider, especially for entities with large footprints.

While the three largest participants in the review conduct or participate in regional exercises which involve several entities arranging simulations of cyber or physical attacks, the remaining participants do not perform larger scale exercises that include their neighbors. However, some participants are made aware of their neighbors' exercises so that they can determine how to coordinate with them.

All participants' system operators participate in semi-annual training, in which they review processes and approaches to responding to larger-scale events that may include cyber attacks. In most cases, the training also provides points of contact for outside

[82] The team also notes that testing of operating plans to address loss of control center functionality, conducted pursuant to EOP-008-1, Requirement R7, may be designed to include aspects of testing of and training on entities' required cyber response and recovery plans, thereby providing the necessary information on interdependencies and vulnerabilities.

agencies and groups that would be involved with large scale or severe events. While some participants have well-established relationships and processes for interfacing with outside groups, others, with less well-defined relationships, have determined that better communication with outside participants is necessary. Many participants also include corporate Incident Response Team members in training exercises on simulated cyber or physical attacks, including training on coordination with outside entities. This practice is especially helpful when a liaison is needed with governmental entities.

Telecommunication infrastructure availability is a particular concern for some participants, as it is critical to their cyber incident response or critical cyber asset recovery plans. In order to test the viability of telecommunications, and ensure personnel readiness for cyber or physical attacks, participants deploy telecommunications support personnel to critical locations during all exercises. Some participants are also considering use of other means of communication, such as mobile radios and emergency-only email portals. In addition, some participants send employees to visit and man their telecom operations center during normal operations to allow employees to test their ability to reach the centers in emergency situations.

3. Related Standards Assessment

Reliability Standards CIP-008-3 and CIP-009-3 include specific requirements addressing drills and exercises to test the viability of a responsible entity's cyber incident response and critical cyber asset recovery plans. The relevant requirements for each standard are as follows:

CIP-008-3:

R1. Cyber Security Incident Response Plan – The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following: …

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans. …

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-009-3:

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident. …

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

Requirement R1.6 of CIP-008-3 requires applicable entities to test their cyber security incident response plan at least annually. Similarly, requirement R2 of CIP-009-3 requires applicable entities to conduct an annual exercise of their critical cyber asset recovery plan. However, these tests or exercises can take the form of a tabletop exercise or paper drill, which may not address the possible circumstances associated with an actual crisis. Tabletop exercises alone do not, in most cases, identify the potential flaws or omissions in the response and recovery plans being tested. By contrast, the joint staff review team found that participation in full operational exercises and other more complex simulation drills provides much greater insight into the viability of a given cyber response and recovery plan, and appears to be necessary to develop robust recovery and response plans.

Participants who took part in regional exercises reported that the exercises were beneficial, resulted in increased situational awareness, and have often led to changes in existing recovery plans and strategies. Each participant stated that engagement in one or more of the exercises and simulations increased their knowledge and awareness of the challenges in responding to a cyber security incident or a cyber or physical attack, resulting in some form of improvement to their recovery plan, notification process, departmental procedures, or communication procedures. In contrast, the team found that a tabletop exercise has limited value and typically does not involve multiple, simultaneous events or issues escalating in severity and duration. Moreover, the team found that tabletop exercises generally do not provide the same opportunity to identify areas for improvement as compared to more complex simulations, and therefore may not result in improvements to the cyber incident and critical cyber asset recovery plans. [83]

[83] Notably, under Reliability Standard EOP-005-2, Requirement R6, an applicable entity must verify that its system restoration plan accomplishes its intended function through analysis of actual events, steady state and dynamic simulations, or other testing. The team found this required verification, along with reliability coordinator review and approval of plans, to be an important element in ensuring that entities develop adequately detailed and thorough system restoration plans.

4. Recommendations

Exercises of response and recovery plans using paper drills. The joint staff review team observed that participation in full operational exercises and other more complex simulations provides greater insight into the viability of a given cyber response and recovery plan, and believes that participation in such exercises by the industry is valuable for developing robust recovery and response plans. The joint staff review team recommends that applicable entities participate in exercise scenarios and simulations structured to gain insight into the viability of cyber response and recovery plans (*i.e.* beyond paper drills and tabletop exercise), including testing for interdependencies and other vulnerabilities.

H. Improving Cyber Security Response and Recovery Plans Based o Actual Events and Other Feedback

1. Summary

The joint staff review team reviewed how participants incorporate feedback and lessons learned from actual cyber security and critical cyber asset recovery events, as well as feedback from other sources regarding the viability of the plans. The joint staff review team found that participants have varying levels of specificity in their processes and procedures for implementing improvements to their cyber security response and recovery plans, including improvements based on lessons learned from actual events. The joint staff review team recommends that further study be conducted about actions being taken by entities when the testing or implementation of their response and recovery plans during actual events reveals the need or opportunity for improvements to the plan.[84] In addition, the study should examine and identify best practices with regard to the types of plan improvements made from entities' analyses of actual cyber events and/or testing. Such information could reveal the need or opportunity for improvements to other entities' response and recovery plans and be a valuable component of a continuous improvement process.

[84] The joint staff review team recognizes that CIP version 5 includes requirements for testing and updating cyber response and recovery plans, but the study could provide additional insight as to how these requirements are working and whether they might be improved.

2. Review of Participants' Response and Recovery Plans

a) Actual Cyber Security Response Events

Most participants that the joint team interviewed were fortunate not to have had an actual cyber security incident that impacted their EMS and SCADA system operations. Some participants have never experienced a cyber threat event that included declaring a cyber security incident involving their critical cyber assets. The joint staff review team believes it is especially important to prepare for cyber security events and incidents by exercising cyber security incident scenarios and participating in drills and exercises that test response and recovery plans and procedures. In this manner, feedback from implementing the plans can drive continuous improvement. Participants indicated, and the joint team agrees, that it is far better to find a flaw in the plans through testing or drills than to discover the issue during an actual event.

b) Actual Critical Cyber Asset Recovery Events

Although not precipitated by cyber threat events, some participants have experienced actual events requiring implementation of their critical cyber asset recovery plans. One of the more common events leading to participants' use of such a recovery plan involves the partial or entire loss of EMS and SCADA systems, which are typically classified as critical cyber assets since they are critical components of bulk power system operations. [85]

Some participants have experienced a complete site loss of their EMS SCADA systems due to extreme weather events (e.g., tornado, fire, floods). [86] Most participants indicated that NERC's Lessons Learned documents analyzing the many EMS and SCADA recovery events have been helpful in improving their critical cyber asset recovery plans,

---

[85] EMS systems, SCADA functions, associated hardware and software, networks, communication systems and supporting systems are a large part of the critical cyber assets that must be addressed in an applicable entity's recovery plan and its objective of restoring control center bulk power system operations.

[86] Response and recovery plans typically include scenarios that address varying levels of loss and interruption of the EMS SCADA system, along with recovery plans and procedures for the mobilization of personnel and activation of alternate control centers. Major disruptions to an EMS and control center operations include loss and unavailability of the EMS system processes, server hardware, or communications, and network availability issues.

by revealing, among other things, interdependencies between cyber assets and systems that were not previously known.[87]

c) Process for Improving Plans

Participants' cyber security response and recovery plans include varying levels of specificity in their processes and procedures for implementing improvements to those plans, including improvements based on lessons learned or information gained during actual events or during testing and drills. Some participants appear to incorporate a feedback loop process used to assess, critique, and direct improvements and changes in a cyber response or recovery plan's procedures and methods based on testing, actual events, or other new cyber threat information.[88]

Participants shared examples of improvements made to recovery plans from exercises, actual events, or new information. A common area for improving recovery plans is in communication processes and methods during emergency conditions. In the event that corporate email communications are interrupted, a separate private emergency email system can be used. In the event a loss of a telecom carriers' Voice over Internet Protocol or mobile communication, an emergency satellite phone system could be implemented. Among other things found from exercising their plans, participants have implemented new procedures and processes for improving formal notification channels or improving coordination efforts with their neighbor entities and Authoritative Agencies.

All participants allow for feedback from all entities involved in a drill or exercise to make suggestions and recommendations to their response and recovery plan. Some participants stated that in their feedback loop (*i.e*, the process used to evaluate performance of their cyber response and recovery plans), certain modifications, improvements, and lessons learned gained during drills and exercises may not rise to the level of a significant change, and therefore may not require modification to their cyber resource or cyber recovery plan. In addition, changes and upgrades in equipment and technology may

---

[87] NERC's Events Analysis program includes a process for developing and issuing "Lessons Learned" documents, intended to ensure the timely dissemination of actionable lessons learned from significant bulk power system events. *See* NERC's Lessons Learned website at http://www.nerc.com/pa/rrm/ea/Pages/Lessons-Learned.aspx .

[88] The joint staff review team found that implementation of a feedback loop can help to correct a plan's procedural mishaps, performance issues in the notification process, communications, and recovery procedures.

require changes to specific recovery procedures and techniques for asset recovery, but will not necessarily result in a change in the overall response and recovery plan.

Another significant feedback area discussed by participants is staying current and active with vendor user support groups and partner relationships with entities that have similar systems. Participants indicated that vendor upgrades and fixes to hardware, software systems, and firmware are not always effectively communicated, or the impact of not implementing the upgrade to systems is not clearly understood. The joint staff review team believes that a feedback process that is part of the overall cyber response and recovery plan can allow for continuous improvements, aid in greater situational awareness and readiness, enhance training programs, shorten response times for cyber events, and fine tune recovery strategies and procedures for such events. Following implementation of response and recovery plans due to an actual event, affected entities should conduct a top to bottom analysis of the event, including identifying any lessons learned that could result in improvements to their (or others') cyber security response or critical cyber asset recovery plans. This analysis should include a determination of whether the actual performance of the response and recovery plan during the test or event indicates that modifications, changes to procedures, and additions and changes to the current response and recovery plans and procedures are needed.

3. Related Standards Assessment

Reliability Standards CIP-008-3 and CIP-009-3 include requirements relating to updates to the cyber security response plan and the critical cyber asset recovery plan, and, as to the latter plan, requiring updates to reflect any changes or lessons learned as a result of an exercise or an actual incident.

CIP-008-3:

R1. Cyber Security Incident Response Plan – The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following: …

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes. …

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-009-3:

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

The joint staff review team found that participants have varying levels of specificity in their processes and procedures for implementing improvements to their existing plans, including improvements and/or updates based on exercises or actual events. The joint staff review team examined the requirements regarding updating plans and actual events, and concluded that currently none require applicable entities to employ a feedback loop or continuous improvement process to ensure that cyber security response and recovery plans are up to date. Although the Reliability Standards do require updating critical cyber asset recovery plans based on lessons learned during testing or during an actual event, these updates tend to be administrative changes in nature (e.g., updating documentation such as personnel contact information) versus including the identification of more substantive plan improvements, most likely due to the fact that drills are typically tabletop exercises. Moreover, the Reliability Standards do not require updating the cyber incident response plan or the critical cyber asset recovery plan whenever new information is acquired that could improve the plans. For recovery and response plans to be effective, they must mimic real life scenarios, be applied to production-like systems, and improve with the ever changing technology. [89]

4. Recommendations

Gain further understanding of response and recovery plan updating follow testing or actual cyber events.

The joint staff review team recommends that a study be conducted to better understand the associated plan improvements made by entities where testing or an actual cyber event reveals the need or opportunity for improvements to a

[89] The team notes that CIP-008-5 Requirement R2, Part 2.2 requires a responsible entity to document any deviations from the written plan that occurred during a response to an incident or an exercise, but does not require an action plan to complete a feedback loop in response to a deviation.

response and recovery plan. This study would support a better understanding of the effectiveness and existence of continuous improvement processes. In addition, the study should examine and identify best practices with regard to the types of plan improvements made from entities' analyses of actual cyber events and/or testing. Such information could reveal the need or opportunity for improvements to other entities' response and recovery plans and be a valuable component of a continuous improvement process.

VI. Appendix 1– Joint Staff Review Team

Federal Energy Regulatory Commission:
Daniel Bogle
Kenneth Githens
Norris Henderson
David Huff
Gilbert Lowe
Raymond Orocco-John
Thomas Reina
Judith Sciullo
Michelle Veloso

North American Electric Reliability Corporation:
Stephen Crutchfield
Tom Hofstetter
Robert Kenyon
Darrell Moore
Katherine Street
Jim Stuart

Northeast Power Coordinating Council, Inc.:
John J. Mosier
Ralph Rufrano

ReliabilityFirst Corporation:
John Idzior
Jeffrey Mitchell

SERC Reliability Corporation:
Steve Corbin
David Greene
Bill Peterson

Western Electricity Coordinating Council:
Darren Nielsen
Tim Reynolds

VII. Appendix 2 –Request Letter for Participation in Reliability Assessmer

Request for Participation in Reliability Assessment

Commission staff, in collaboration with NERC and the Regional Entities, is initiating a voluntary review of recovery and restoration plans for selected registered entities. The purpose of this joint staff review is to assess and verify the electric utility industry's bulk power system recovery and restoration planning, and to test the efficacy of the relevant Reliability Standards in achieving or maintaining reliability. The joint staff review is focused on supporting entities in ensuring reliable restoration from reliability events and reviewing the adequacy of the Reliability Standards; it is not a compliance and enforcement initiative.

Recent reliability events, including weather-driven events (e.g., Superstorm Sandy, February 2011 Southwest cold weather rolling blackouts), bulk power system disturbances (e.g., September 2011 Arizona-Southern California Blackout, 2008 Florida Blackout, 2003 Northeast Blackout) and possible cyber/physical attacks have highlighted the potential to cause widespread adverse effects on the bulk power system. Effective system recovery and restoration plans are essential to facilitate a quick and orderly recovery in the aftermath of such events.

The primary objective of this joint staff review is to assess entities' plans for restoration and recovery, and verify how the Reliability Standards support them. To accomplish this objective, the joint staff review will:

- Gather information via outreach with a representative sample of selected entities with significant bulk power system responsibilities.
- Understand the overall state of restoration plans by comparing and contrasting their content, scope and interrelationships.
- Assess the clarity of the Reliability Standards in supporting the adequacy and efficacy of restoration and recovery plans.
- Identify good industry practices or make recommendations to ensure that effective restoration and recovery plans are in place to support reliability.

As an entity with bulk power system significance and broad interrelationships that may impact restoration planning, we are requesting [ENTITY]'s participation in this review. Additionally, other registered entities with interrelated reliability functions that impact, or are impacted by, [ENTITY]'s restoration plan may also be asked to participate in order to achieve comprehensive review of the wider area restoration capabilities.

The focus on the recovery and restoration plan review will be based on the reliability intent of three Reliability Standards:

EOP-005-2 System Restoration Plans from Blackstart Resources[1]
CIP-008-3 Cyber Security — Incident Reporting and Response Planni
CIP-009-3 Cyber Security — Recovery Plans for Critical Cyber Assets

Specifically, documents and information to be requested during the entity outreach, depending on their applicable functions, will include:

- Reliability Coordinator approved restoration plan
- Procedures for deploying blackstart resources
- Selected results of the most recent analysis of actual events, steady state and dynamic simulations, and testing that the restoration plan accomplishes its intended function, including any restoration strategies used to facilitate restoration for recent disturbances or the deployment of blackstart resources
- Existing notes or recommendations recorded as a result of the most recent annual exercise or from an actual incident. Also, any Reliability Coordinator feedback or analysis of last year's system restoration drills, exercises or simulations, as dictated by the particular scope of the drills, exercises, or simulations that were conducted [2]

[1] The assessment of EOP-005 will also consider the NERC report "Standards Independent Experts Review Project; An Independent Review by Industry Experts." Located at and accessed April 1, 2014: http://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/Standards_Independent_Experts_Review_Project_Report.pdf

[2] The provided documents may be informative on how other activities required by the above or related Reliability Standards are accomplished (e.g. EOP-006-2 – System Restoration Coordination). In some cases, other information as it relates to the above or

- Cyber Security Incident Response Plan
- Recovery Plan(s) for Critical Cyber Assets

The joint review will also assess entities' reports or recommendations from major events to understand the effectiveness of their recovery and restoration plans following an actual implementation. Reports developed after actual events like Hurricane Sandy, the September 2011 Arizona-Southern California Blackout, the Derecho storms in the Midwest and Mid Atlantic in 2012, and the 2014 Polar Vortex are also requested in order to better put response, recovery and restoration plans into the context of overall reliability efforts. The joint staff review will also use any public or private reports that have already been produced in these areas.

In addition to the information specified above, entities are encouraged to provide any further information or documents that may be helpful in explaining their recovery and restoration planning.

This collaborative assessment by the Commission, NERC and the Regional Entities is an important step in protecting reliability by gauging the electric utility industry's level of preparation for a major event and the ability to recover quickly and efficiently. In anticipation of [ENTITY]'s participation, we thank you and will work closely with you to ensure this project is conducted as a partnership with minimal disruption to your organization. I or my staff will call you at your earliest convenience to provide greater detail and answer any questions or concerns that you may have about this joint staff review.

---

other Standards may be requested later, as needed, in order to have a complete understanding of the applicable entity's restoration and recovery processes.

VIII. Appendix 3 – Standards and Requirements Assessed

EOP-005-2 – System Restoration from Blackstart Resources

In accordance with the scope of the review, Requirements assessed included the restoration plan-related requirements, as well as any requirements that support how the applicable entities test the effectiveness of their plans. These Requirements are listed below.

Reliability Coordinator-Approved Restoration Plan:[1]

R1. Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include:

R1.1. Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.

R1.2. A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.

R1.3. Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.

[1] See Appendix 2 - Request Letter for Participation in Reliability Assessment, which provides the scope of review.

R1.4. Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.

R1.5. Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

R1.6. Identification of acceptable operating voltage and frequency limits during restoration.

R1.7. Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.

R1.8. Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.

R1.9. Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.

R4. Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan.

R4.1 Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval within the same 90 calendar day period.

R13 Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements.

Selected results of the most recent analysis of actual events, steady state dynamic simulations, and testing that the restoration plan accomplishes i

intended function, including any restoration strategies used to facilitate restoration for recent disturbances or the deployment of [2] ***blackstart resou***

R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify:

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.

R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.

R9. Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include:

R9.1 The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.

R9.2 A list of required tests including:

R9.2.1 The ability to start the unit when isolated with no support from the `BES or when designed to remain energized without connection to the remainder of the System.

R9.2.2 The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be

[2] See Appendix 2 - Request Letter for Participation in Reliability Assessment, which provides the scope of review.

energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.

R9.3. The minimum duration of each of the required tests.

Existing notes or recommendations recorded as a result of the most recer exercise or from an actual incident. Also, any Reliability Coordinator feedl analysis of last year's system restoration drills, exercises or simulations, the particular scope of the drills, exercises, or simulations[3] that were cond

R10. Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following:

R10.1. System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.

R10.2. Restoration priorities.

R10.3. Building of cranking paths.

R10.4. Synchronizing (re-energized sections of the System).

R12. Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator.

R18. Each Generator Operator shall participate in the Reliability Coordinator's restoration drills, exercises, or simulations as requested by the Reliability Coordinator.

CIP-008-3 — Cyber Security — Incident Reporting and Response Planning

[3] See Appendix 2 - Request Letter for Participation in Reliability Assessment, which provides the scope of review.

In accordance with the scope of the review, Requirements assessed included the cyber security incident response plan-related requirements, as well as any requirements that support how the applicable entities test the effectiveness of their plans. These Requirements are listed below.

Cyber Security Incident Response Plan:[4]

R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.

R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.

R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.

R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.

R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-009-3 — Cyber Security — Recovery Plans for Critical Cyber Assets

[4] See Appendix 2 - Request Letter for Participation in Reliability Assessment, which provides the scope of review.

In accordance with the scope of the review, Requirements assessed included the critical cyber asset recovery plan-related requirements, as well as any requirements that support how the applicable entities test the effectiveness of their plans. These Requirements are listed below.

Recovery Plan(s) for Critical Cyber Assets:[5]

CIP-009-3:

R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.

R4. Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

---

[5] See Appendix 2 - Request Letter for Participation in Reliability Assessment, which provides the scope of review.

IX. Appendix 4 – Glossary of Terms Used in Report

Advanced Persistent Threat: A set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity.

Alternating Current (AC): Current that changes periodically (sinusoidally) with time.

Area Control Error (ACE): The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, plus the instantaneous difference between the interconnection's actual frequency and scheduled frequency and a correction for meter error.

Automatic Generation Control (AGC): A feature of a power system's centralized control system that automatically adjusts generation in a Balancing Authority Area to maintain the Balancing Authority's interchange schedule plus its frequency bias.

Balancing Authority: The responsible entity that integrates resource plans ahead of time, maintains load-interchange-generation balance within a Balancing Authority Area, and supports Interconnection frequency in real time.

Balancing Authority Area: The collection of generation, transmission, and loads within the metered boundaries of the Balancing Authority. The Balancing Authority maintains load-resource balance within this area.

Blackstart Resource: Generating unit and associated equipment with the ability to be started without support from the Bulk Electric System (BES) or is designed to remain energized without connection to the remainder of the BES, with the ability to energize a bus, meeting the transmission operator's restoration plan needs for real and reactive power capability, frequency and voltage control, and that have been included in the transmission operator's restoration plan.

Bulk Electric System (BES): The electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher.

Business Continuity Plan: Includes procedures for sustaining mission/business operations while recovering from a significant disruption.

Cascading: The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.

Cranking Path: A portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other generating units.

Critical Asset: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Critical Cyber Asset: Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident: Any malicious act or suspicious event that compromises, or attempts to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset; or disrupts, or attempts to disrupt, the operation of a Critical Cyber Asset.

Direct Current (DC): Electric current that is steady and does not change in either magnitude or direction with time. DC is also used to refer to voltage and, more generally, to smaller or special purpose power supply systems utilizing direct current either converted from AC, from a DC generator, from batteries, or from other sources such as solar cells.

Disaster Recovery Plan: A plan that provides procedures for relocating information systems operations to an alternate location.

Distribution Provider: Provides and operates the “wires” between the transmission system and the end-use customer. For those end-use customers who are served at transmission voltages, the transmission owner also serves as the distribution provider. Thus, the distribution provider is not defined by a specific voltage, but rather as performing the distribution function at any voltage.

Extra High Voltage (EHV): Transmission lines with voltages above 765 kV.

Generator Operator: The entity that operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services. The generator operator is responsible to have procedures for starting each blackstart resource, in accordance with Reliability Standard EOP-005-2.

Generator Owner: The entity that owns and maintains generating units. Generator owner plant control room personnel also play a role in restoration.

Incident Response Teams: Responsible personnel designated in the cyber security response plan assigned to respond to a Cyber Security Incident or a detected cyber threat event.

Intrusion Detection System: Either a hardware or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

Intrusion Prevention System: Network security appliances that monitor network and/or system activities for malicious activity.

Island, Electrical: An electrically isolated portion of an interconnection. The frequency in an electrical island must be maintained by balancing generation and load in order to sustain operation. Islands are frequently formed after major disturbances wherein multiple transmission lines trip, or during restoration following a major disturbance.

Isochronous Governor Control: An isochronous (or zero droop) governor maintains the same speed regardless of the load, and ensures that the frequency of the electricity generated is constant or flat. Isochronous control mode is used to control frequency in an island during system restoration.

Network Operations Center: One or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication or satellite network.

Phasor Measurement Unit (PMU): Device that measures the electrical waves on an electricity grid, using a common time source for synchronization.

Reactive Power: The portion of electricity that establishes and sustains the electric and magnetic fields of AC equipment. Reactive power must be supplied to most types of magnetic equipment, such as motors and transformers. It is also needed to make up for the reactive losses incurred when power flows through transmission facilities. Reactive power is supplied primarily by generators, capacitor banks, and the natural capacitance of overhead transmission lines and underground cables (with cables contributing much more per mile than lines). It can also be supplied by static VAr compensators and other similar equipment utilizing power electronics, as well as by synchronous condensers. Reactive power directly influences system voltage such that supplying additional reactive power increases the voltage. It is usually expressed in kilovars (kvar) or megavars (Mvar), and is also known as “imaginary power.”

Regional Entity: An independent, regional entity with delegated authority from NERC to propose and enforce Reliability Standards and to otherwise promote the effective and efficient administration of bulk power system reliability.

Registered Entity: An entity that is a user, owner, or operator of the bulk power system that is generally required to register with NERC.

Regulation: The ability to maintain a quantity within acceptable limits. For example, frequency regulation is the control or regulation of the system frequency to within a tight

bandwidth around 60 Hz. Voltage regulation is the control of a voltage level within a set bandwidth. In power systems operations, regulation often refers broadly to changing the output level of selected generators to match changes in system load.

Reliability Coordinator: The entity that is the highest level of authority who is responsible for the reliable operation of the Bulk Electric System, has the Wide Area view of the Bulk Electric System, and has the operating tools, processes and procedures, including the authority to prevent or mitigate emergency operating situations in both next-day analysis and real-time operations. The reliability coordinator has the purview that is broad enough to enable the calculation of Interconnection Reliability Operating Limits, which may be based on the operating parameters of transmission systems beyond any Transmission Operator's vision.

Restoration: The process of returning generators and transmission system elements and restoring load following an outage on the electric system.

Security Information and Event Management: Term for software products and services combining security information management (SIM) and security event management (SEM). This technology provides real-time analysis of security alerts generated by network hardware and applications. It is sold as software, appliances or managed services, and is also used to log security data and generate reports for compliance purposes.

Static VAr Compensators: A combination of shunt reactors and shunt capacitors with switching that is precisely controlled by power electronics to automatically manage reactive power injections and withdrawals from the power system to help maintain proper transmission voltage.

Supervisory Control and Data Acquisition (SCADA): A system of remote control and telemetry used to monitor and control the transmission system.

Synchronize: The process of bringing two electrical systems together by closing a circuit breaker at an interface point when the voltages and frequencies are properly aligned. Also, when generators are brought on-line, they are said to be synchronized to the system.

Synchronous: To be in-step with a reference. The rotor of a synchronous machine, be it a motor or a generator, spins in unison with the power system in terms of frequency.

System Operator: An individual at a control center of a balancing authority, transmission operator, or reliability coordinator, who operates or directs the operation of the bulk electric system (BES) in real-time.

System Restoration Plan: Plan required to allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk

Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System.

Thyristors: Semiconductor devices that act as switches.

Transmission Operator: The entity responsible for the reliability of its "local" transmission system, and that operates or directs the operations of the transmission facilities. The transmission operator is required to have a restoration plan, in accordance with EOP-005-2.

Transmission Owner: The entity that owns and maintains transmission facilities. The transmission owners identified in the transmission operators' restoration plans are required to provide system restoration training to their field switching personnel identified as performing unique tasks associated with the transmission operators' restoration plans, in accordance with EOP-005-2.

Voltage Source Converter: Semiconductor devices that act as switches in the converter but function differently from thyristors. Commutation during the inversion process (DC to AC at the receiving terminal) will take place under all system conditions at the receiving end. This allows a voltage source converter to be used when the system is very weak or blacked out.

X. Appendix 5 - Acronyms Used in Report

AC	Alternating Current
ACE	Area Control Error
AGC	Automatic Generation Control
ALR	Automatic Load Rejection
BES	Bulk Electric System
CIP	Critical Infrastructure Protection Reliability Standards
COM	Communications Reliability Standards
DC	Direct Current
EHV/HV	Extra High Voltage/High Voltage
EOP	Emergency Preparedness and Operations Reliability Standards
EMS	Energy Management System
E-ISAC	Electricity Information Sharing and Analysis Center
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
Hz	Hertz
ICCP	Inter-Control Center Communications Protocols
IERP	Independent Experts Review Project
IRO	Interconnection Reliability Operations and Coordination Standards
kV	Kilovolt
MVA	Megavolt Ampere
MW	Megawatt
NERC	North American Electric Reliability Corporation
PER	Personnel Performance, Training, and Qualifications Reliability Standards
PMU	Phasor Measurement Unit
PRC	Protection and Control Reliability Standards
SCADA	Supervisory Control and Data Acquisition
TOP	Transmission Operations Reliability Standards
UFLS	Underfrequency Load Shedding
VAr/MVAr	Volt Ampere reactive/Mega-Volt-Ampere reactive