

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Evaluation of the Physical Security Reliability Standard) And Physical Security Attacks to the Bulk-Power) System.)	Docket No. RD23-2-000
Sixth Meeting of the Joint Federal-State Task Force) On Electric Transmission)	Docket No. AD21-15-000

**MOTION TO INTERVENE AND COMMENT OF THE
SECURE-THE-GRID COALITION
(submitted to FERC on May 15, 2023)**

Pursuant to Rules 206, 212, and 214 of the Rules of Practice and Procedure¹ of the Federal Energy Regulatory Commission (hereafter “FERC” or “Commission”) and the FERC Notice in Docket No. RD23-2-000 and Docket No. AD21-15-000, the Secure-the-Grid Coalition (“Coalition”) [which is sponsored by the Center for Security Policy - a non-profit 501(c)(3) organization] which is engaged in research and public education to strengthen the resilience of critical infrastructures, files this Motion to Intervene and Comment in support of (1) expanding the Applicability criteria set forth in the Physical Security Reliability Standard; (2) improving the required risk assessment set forth in the Physical Security Reliability Standard; and (3) coming to an actionable decision upon a minimum level of physical security protections that should be required for all BPS substations and their associated primary control centers.

The Secure-the-Grid Coalition (“Coalition”) has previously commented before the Federal Energy Regulatory Commission (“FERC” or “Commission”) on Physical Security Standard CIP-14. More than three years ago, our Motion to Intervene in Docket No. AD20-21 was authored by Coalition Co-Chairman Ambassador R. James Woolsey, former Director of Central Intelligence. In that motion, Ambassador Woolsey correctly stated that:

“The complaint which initiated this docket points out numerous loopholes in the established physical security standard (CIP-014-2) and the fact that there have been only 4 citations issued for violations of the standard – all for administrative violations – in the six years since it was established. I want to commend your Commission for opening this docket after receiving that complaint and I want to encourage you to take this opportunity to deeply analyze the effectiveness and the enforcement of the physical security standard you previously approved

against the current threat environment and the reality that our modern civilization depends entirely upon the bulk power system which you regulate.”¹

“Americans witness daily the unguarded status of critical electric utility assets, as do our enemies. A growing number of Americans are beginning to understand why these assets remain so vulnerable.”²

The Coalition commends the FERC Commissioners for opening these two dockets, AD21-15-000 and RD23-2-001 to review the adequacy of current Physical Security Standard CIP-014-003.

Earlier today the Coalition filed with FERC a Petition for Rulemaking on an “Enhanced Standard for Determining Critical Infrastructure, Using Engineering Models to Define Critical Infrastructure Assets to be Subject to Enhanced Protections” (“Petition”). The Coalition has filed this Petition in addition to a previous filing in 2019 by Michael Mabee, a Coalition member,³ which failed to receive a response from FERC, contrary to Administrative Law.⁴

The Coalition wishes to commend many of the participants of the Sixth Meeting of the Joint Federal-State task force (“Task Force”) which met last February. Sitting members of the Task Force include all FERC Commissioners and 10 regionally selected state utility commissioners. At the 6th Meeting of the Task Force, two special guests were invited to present and field questions: Mr. Jim Robb, President of North American Reliability Corporation (“NERC”), and Mr. Puesh Kumar, Director, Office of Cybersecurity, Energy Security, and Emergency Response (“CESER”).

The Coalition wishes to commend FERC Chairman Phillips for bringing the urgency of guarding against ballistic attack of electric substations into focus during his opening statement by observing that the increase of ballistic incidents against substations in 2022 “drastically” outpaced the increase in ballistic incidents overall.⁵

¹ Woolsey, Ambassador R. James, Co-Chairman of Secure-the-Grid Coalition. “Motion to Intervene by Secure the Grid Coalition” under EL20-21. (March, 2020)

https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20200303-5075 (accessed May 14, 2023)

² Ibid.

³ Mabee, Michael, “Petition for Rulemaking to Require Disclosure of Names of Regulated Entities Subject to Regulatory Actions by the Commission or by the Electric Reliability Organization” (2019)

<https://michaelmabee.info/wp-content/uploads/2019/02/Petition-for-Rulemaking-Mabee-with-exhibits-1.pdf> (accessed May 15, 2023)

⁴ Administrative Procedure Act § 553 - Rule making, <https://www.archives.gov/federal-register/laws/administrative-procedure/553.html>

⁵ “Sixth Meeting of the Joint Federal-State Task Force on Electric Transmission” video at <https://ferc.gov/news-events/events/sixth-meeting-joint-federal-state-task-force-electric-transmission-02152023> (accessed May 14, 2023)

Moreover, the Coalition would like to commend the Joint Federal-State Task Force on Electric Transmission for its work to date, and it is our wish that the Joint Task Force existence is extended beyond its current three-year life, which ends in a matter of months. The formal collaboration and sharing of problems and airing of disputes among the varied regions is quite suited as a keystone forum in activating and informing on the prescriptions for enhanced Physical Security protections explained in the Coalition's requested Prescriptive Actions.

Background

Michael Mabee, the same person mentioned above, who had his Petition for Rulemaking neglected, contrary to administrative law, filed a different, formal Complaint with FERC on the inadequacy of CIP-014 on January 29, 2020, which opened docket EL20-21-000.⁶ Complainant followed with "Additional Information and Recommendations of Complainant," filed on February 19, 2020.⁷

Mr. Mabee's Complaint dealt with many of the physical security issues we face today. We believe that if there had been adequate action on this Complaint by the previous FERC Commissioners, that this issue would not be necessary to focus upon so intently by the current sitting Commissioners, since many of the physical vulnerabilities of the electric grid could have been remedied.

As it was, EL20-21-000 was dismissed by FERC.

One such point in the Mabee Complaint was the issue of considering simultaneous loss of multiple facilities, most often referred to as "coordinated attacks," or "N-2, N-3, N-4," etc., which means multiple, simultaneous attacks against more than one substation. This is now a scenario that is being considered.

As NERC President Robb stated during the Task Force Meeting of February, 2023:

"As I said, I think the thing that we need to chew on collectively is, you know, is the loss of a single element of the system the right test? Or do we need to be thinking more about multiple elements given this observation that we have at least one bona fide coordinated attack being planned, which is the one in Baltimore. I don't know all the specifics around Moore County, to

⁶ Mabee, Michael, "Complaint under Section 215 of the Energy Policy Act of 2005 related to CIP Standards," filed on January 29, 2020, https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20200130-5256 (accessed May 14, 2023)

⁷ Mabee, Michael, "Additional Information and Recommendations of Complainant," filed on February 19, 2020, https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20200219-5161 (accessed May 14, 2023)

*know how much insight the individuals there had into the grid that they were attacking, and even less in the Seattle Tacoma area. So there's more insight to be gained out of those events, but I think the question around **defense against coordinated attack has to be something that's on the table.**" [emphasis added]⁸*

Yet, NERC's April 2023 Report repeatedly states that they do not recommend expansion of CIP-014-000.

The Coalition notes that NERC President Robb also stated during the February, 2023 Task Force Meeting:

"I think one question that's clear on the table has to be whether or not the risk assessments should continue to focus only on the loss of a single asset, an N minus 1 condition, or should we look at the situations where more than one asset is taken out? "The coordinated attack." You know, that's kind of what we saw happen in Baltimore, as we understand it, and a bit of a situation we had in North Carolina. So the question is should it still be a single contingency, or should we look at multiple contingencies from a risk assessment?"⁹

Again, the April, 2023 NERC Report proposes no expansion of CIP-014-003, but instead suggests a future "Technical Conference" to consider this.¹⁰

President Robb also stated the following on Risk Assessment at the Task Force Meeting:

"Second, should the risk assessment be focused primarily on the prevention of a major cascading outage, or should we somehow figure out how to incorporate appropriately the concept of customers impacted, given society's growing dependence on electricity?"¹¹

Meanwhile, the April 2023 NERC Report continuously states that there is no reason to expand CIP-014 at this time, but that NERC will continue to consider vulnerabilities and impacts and of course hold a technical conference.¹²

NERC President Robb also stated the following on Costs versus Protection:

"Third, right, how should the mitigation plans best optimize between investment and protective measures, versus investment in the ability to arrest and restore and recover from an event. And then finally, I guess this is a very appropriate thing for this audience, is there a way through our standards to create the framework for a more direct dialogue between the utilities and the state regulators who will have to approve cost recovery for any investments that are made around the

⁸ Op. Cit. "Sixth Meeting..."

⁹ Ibid.

¹⁰ "Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System," North American Electric Reliability Corporation, April 14, 2023, page 5.
<https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20Report%20on%20CIP-014-3.pdf> (accessed May 14, 2023)

¹¹ Op. Cit. "Sixth Meeting..."

¹² Op. Cit. "Evaluation of the Physical Security Standard..."

risks that's embedded in their systems, the costs to mitigate that risk, versus the cost to recover, and have a collaborative conversation around how much risk are you willing to wear, versus how much do we want to mitigate. And when we mitigate, do we want to do that through prevention or recovery?"¹³

Recovery simply means that your protection scheme has either failed, was absent, or was insufficient.

President Robb also conveys his concept of impact on the system to date from physical attack, stating that there has been almost none, and "You know, it takes an awful lot to damage equipment to the point where it can't function." It is certain that Mr. Robb is aware, as are every power engineer and field technician everywhere in the world, and many laypersons are as well, that a single bullet penetration can permanently damage extremely expensive equipment that takes a very long time to replace. The costs of adding effective ballistic shielding to these high-value target areas are miniscule in comparison to the purchase price of the assets or the cost to society of losing electricity. In terms of value to the impacted communities, the cost to protect these assets is infinitesimal.

Applicability

Among the CIP-014-003 questions FERC has posed regard the determinants of "Applicability." As mentioned previously, the Coalition has earlier today filed a Petition for Rulemaking, and by this reference, that petition, filed May 15, 2023, is made part of this motion to intervene and comment as **"Enclosure 1."**

That petition was informed to a great extent by a recent article authored by a power engineer of career length experience in the electric utility industry. That article is incorporated into aforementioned Petition as "Exhibit D."¹⁴

The theme of the petition is that FERC should order an enhanced applicability standard that:

¹³ Op. Cit. "Sixth Meeting..."

¹⁴ Swearingen, Michael T., "Plausible Deniability Rather Than Pragmatic Solutions the Signature of NERC CIP" May 11, 2023, <https://securethegrid.com/plausible-deniability-rather-than-pragmatic-solutions-the-signature-of-nerc-cip/> (accessed May 15, 2023)

- (1) Requires the regional authorities to use their amalgamated operating models to designate the critical assets that ensure the reliable flow of power, and lessen the risk of uncontrolled separation, instability, or cascading outages.
- (2) Requires the industry to establish new metrics for Risk Assessments that incorporate real-world factors pertaining to the risks associated with physical sabotage, such as known asset vulnerabilities, attacker capabilities, and attacker intentions. [One known “asset vulnerability” should be whether an applicable asset (such as a large power transformer) is vulnerable to ballistic attack and currently unprotected against such an attack.]

In addition to the Petition, our Coalition also suggests FERC work with the National Guard Bureau to promote the concept of “Red-Teaming” for the purpose of spot checking of utilities for compliance with the new expanded physical protection standard.

National Guard units located in every state of the Union possess experts in physical security and these units have an incentive to help make sure that the grid doesn’t suffer an outage due to physical attack since the Guard would be burdened with responding to the subsequent blackout. Were FERC to collaborate with the Guard Bureau to express support for this concept, it would give lower-level commanders a better justification to work directly with the utilities in their states.

“Red-Teaming” by the National Guard would provide at least some assurance against one of many “loopholes” Michael Mabee pointed out in his submission of “Additional Information and Recommendations of Complainant” in EL20-21-000:

This “unaffiliated third party” can still be a peer Transmission Owner who meets the criteria of R6.1 (which most probably do). This means that peer Transmission Owners could verify each other’s evaluations (R4) and physical security plans (R5). This creates an obvious conflict of interest and could incent an “unaffiliated third party” to “go easy – they are reviewing us next week.”¹⁵

Moreover, the practice of having the National Guard step in as an “unaffiliated third party,” if followed, would provide an additional benefit to the state involved, insofar as the executive branch in the state

¹⁵ Op. cit., Mabee, Michael, “Additional Information and Recommendations of Complainant,” page 8.

and the state and county emergency management personnel would have an improved view of what to expect, and what to plan for under an expanded set of adverse conditions.

Risk Assessment

As is generally known in security matters, and is acceptably valid in this case, is the difference between what is referred to as a “risk assessment” and what is referred to as a “threat assessment.” The risk assessment, to many professionals refers to the type of metric that a property casualty insurer might use that focuses weight on two types of factors, one is “frequency of occurrence,” and the other is “consequence” or “extent of damage.”

But now, because of the thwarted conspiracy in Maryland, it is finally recognized within the electric energy complex that a planned coordinated effort, of the kind that the alleged conspirators, Sarah Beth Clendaniel and Brandon Clint Russell plotted, requires an expanded metric from that which is commonly referred to as a “risk assessment.”

A threat assessment metric adds the factors of intentions (of actors) and capabilities (of actors) and vulnerability (of systems in need of protection) to the consequence aspects.

While NERC does not see any reason to expand CIP-014-003, NERC is willing to at least countenance the broadening of this aspect of physical security of substation and other transmission assets against attacks from sophisticated actors through use of “Design Basis Threat” risk assessments that consider motivations, capabilities, and tactics of an adversary as well as the frequency and the consequence. At least it will be discussed at a tabletop exercise, which is an improvement.

One item to also consider is that “frequency,” as used in any risk assessment metric, is not synonymous with “probability.” bIn simplified terms, a true threat assessment that would benefit the electric power complex on the matter of physical security threats would be:

Threat = Intentions x Capabilities x Vulnerabilities x Consequence.

Calling for Prescriptive Action

Utilities not subject to FERC jurisdiction concerning electric rates are subject to the utility regulatory authority established by the states. However, FERC certification of NERC as the ERO subject to FERC oversight allows for the NERC Standards CIP-002-5 BES Cyber System Categorization and CIP-014-3 Physical Security to be expanded to include critical infrastructure based on the system models of the RTO's, ISO's and other transmission reliability authorities. Should these models include distribution facilities and other non-jurisdictional facilities, such facilities can be subject to expanded CIP-002-5 and CIP-014-3 standards.

The Secure-the-Grid Coalition respectfully requests FERC, as the ultimate Electric Reliability Organization, expand the Physical Security Standard to define as critical those substations that comport, at minimum, with those nodes recognized as critical nodes in engineers' operational models from each Registered Entity that are amalgamated at the RTOs, ISOs, ERCOT, and other reliability (Generation and Transmission) authorities. Thus, as a matter of engineering, critical nodes are better identified than under the current Applicability standard which is unwieldy and has been confusing. These designated critical nodes require prioritization for enhanced defensive steps, to include hardware installation (such as ballistic protection) to counter damage or destruction, and thereby avoid uncontrolled separation, instability, and cascading outages from physical attack.

Therefore, our Coalition recommends that (1) FERC prescribe that the electric industry use operating engineering models to identify the "critical nodes" and (2) that the industry be required to install protective ballistic barriers to substation equipment assets:

- 1 that cannot be replaced or repaired within a 45-day time frame and cost more than \$500,000 to replace will need to be protected by anti-ballistic shielding; and
- 2 that such shielding can be provided by layout of the pad in such a way that the targeted areas of the asset, capable of instant destruction of the asset are not in a visual line-of-sight from outside the fence perimeter from all angles. Other means of shielding from line-of-sight from all angles

of the substation, for example could be the control house itself, which falls under the layout of the substation pad category; and

- 3 that all high value target surfaces (as designated above), that are visible line of sight from even one angle outside of the fenced perimeter space would be required to have ballistic shielding to stop ballistic penetration. That shielding can be in the form of jersey barriers, Kevlar ballistic curtains (fabric), ballistic fiberglass panels, or metallic panels capable of stopping penetration of high caliber rifle fire; and
- 4 that the certification process that exists within the current standard CIP-014-003 is acceptable in the new standard, subject to one qualification, which is that on a recurring basis, at least annually, at least one utility within each state will be spot checked using unaffiliated “Red Teams” – such as those which could be employed by the state’s National Guard units.

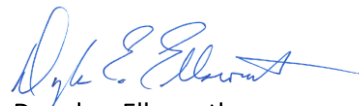
Conclusion

The Secure-the-Grid Coalition appreciates the opportunity to address this issue of extreme importance. We sincerely hope that the prescriptions offered herein get more attention as Commissioner Christie so correctly observed, “So I hope this prioritization issue continues to get more attention, and again, I wish Jim [Robb] were here to tell us about where's the gap in CIP-14 about who makes that decision. It's really important to get that right.”¹⁶ Indeed, it is important to get that right. If we do not get it right this time, we expect the most optimistic conclusion is that we will be back again to discuss this matter in another three years, or less...depending. The more realistic and pessimistic conclusion is that we will suffer more power outages and of longer duration due to physical attacks on our presently vulnerable electric grid.

Respectfully submitted,



Thomas J. Waller Jr.
Co-Director
Secure-the-Grid Coalition
twaller@centerforsecuritypolicy.org



Douglas E. Ellsworth
Co-Director
Secure-the-Grid Coalition
doug.ellsworth@usapact.org

¹⁶ Transcript “Sixth Meeting of the Joint Federal-State Task Force on Electric Transmission” February 15, 2023 (attached as Exhibit), p. 84.

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

Petition for Rulemaking to Require an Enhanced Standard for Determining Critical Infrastructure, Using Engineering Models to Define Critical Infrastructure Assets to be Subject to Enhanced Protections)
)
) **Docket No. _____**
)
)
Secure-the-Grid Coalition, Petitioner)

Submitted to FERC on May 15, 2023

Under procedures set forth in 18 CFR 385.207 – *Petitions (Rule 207)*, the Secure-the-Grid Coalition (“Petitioner”) respectfully submits a Petition for Rulemaking for a rule of general applicability, consistent with Commission authority for electric reliability under Section 215 of the Federal Power Act.¹ We ask the Federal Energy Regulatory Commission (“FERC” or “the Commission”) to order the North American Electric Reliability Corporation (“NERC”) to set an enhanced standard to be used in the determination of critical infrastructure that would be subjected to evaluation through the use of most recently updated engineering models used in operations for the purpose of determining which assets, if damaged, permanently destroyed, or otherwise rendered inoperable, would lead to uncontrolled separation, cascading outages or instability.

FERC Rule § 385.207 - Petitions (Rule 207) provides:²

(a) General rule. A person must file a petition when seeking:

- (1) Relief under subpart I, J, or K of this part;
- (2) A declaratory order or rule to terminate a controversy or remove uncertainty;
- (3) Action on appeal from a staff action, other than a decision or ruling of a presiding officer, under Rule 1902;
- (4) A rule of general applicability; or
- (5) Any other action which is in the discretion of the Commission and for which this chapter prescribes no other form of pleading.

¹ 18 C.F.R. § 39.2(d) (2021) (the ERO “shall provide the Commission such information as is necessary to implement section 215 of the Federal Power Act”).

² 16 U.S.C. § 824o.

Petitioner recognizes that this petition for rulemaking is for a rule of general applicability; hence it is requested under authority of Commission Rule 207(a)(4). Petitioner recognizes that action by the Commission under Rule 207(a)(4) is by the discretion of the Commission.

The Commission has a duty under Section 215 of the Federal Power Act to approve and enforce reliability standards to provide for reliable operation of the Bulk Power System. For cybersecurity, FERC authority is at its apex; Section 215 gives FERC specific authority to regulate the Bulk Power System for physical protection.

We appear now before the Commission to request expedited addition of enhanced Applicability Criteria to the existing system of reliability standards for the Bulk Power System. Accumulating evidence in the public domain shows that electric grids—and the critical infrastructures that depend upon reliable power—are increasingly at risk from direct physical attack. Due to the grave and immediate threat of widespread, long-term blackouts enabled by successful and coordinated physical damage or destruction, we request that the Commission develop a framework for an enhanced Physical Security Standard and thereafter issue to NERC an “Order Directing the Filing of Standards,” with a deadline of no more than 90 days for submission of a proposed standard.

Background - Vulnerability of Critical Electric Assets in Substations

Recent media coverage of acts of vandalism and sabotage have heightened public awareness to the vulnerability of critical assets that are not protected against ballistic attack. The list of media articles and videos is long and includes well-known and popular outlets ranging from the Wall Street Journal to Newsweek, to ABC’s 60-Minutes. Despite the recent “outbreak” of media attention to physical sabotage against electric substations, the targeting of electric grid equipment by criminals, thieves, and saboteurs has a long history. Data provided to the Department of Energy via its OE-417 reports demonstrate that physical attacks happen at a frequency of more than one per week across the North American electric grid. [From January 1, 2010, through August 2022, there were at least 919 physical attacks on the U.S. grid and the rate of attacks is increasing.]³

³ <https://securethegrid.com/north-carolina-blackout-highlights-growing-grid-security-problem/>

Also, according to NERC President Jim Robb, speaking at the **Sixth Meeting of the Joint Federal-State Task Force on Electric Transmission (JFSTFET) on February 21, 2023**:

“Typically we’ve seen vandalism, break-ins, you know, geared around theft, and so forth. It’s really been over the last several years. I mean there’s always been kind of like we could always refer to them as the drunk hunters, right, that will go out and will fire at electric equipment. But what we’ve seen over the last several years clearly there’s been an increase in ballistic activity, and in step with clearly intent to harm equipment as opposed to whatever else might motivate someone to do this work.”⁴

[**Exhibit A** is a full transcript of this meeting.]

It is important to note that others in attendance at the Sixth Meeting of the JFSTFET advised that majority of these historical cases did not result in prolonged outages. The reason for this is that the assailants either lacked the intent to do permanent damage or were not sophisticated enough to aim at a targeted area that would cause permanent damage to long-lead-time critical assets.

Increased Sophistication of Attackers

A Criminal Complaint (**Exhibit B**) was filed in the United States District Court for the District of Maryland on February 2, 2023, under 18 U.S.C. 1366, described as “**Conspiracy to Destroy an Energy Facility.**” [Case No. 23-mj-00401-MJM, United States of America v. Sarah Beth Clendaniel and Brandon Clint Russell]

A reading of the Section pertaining to the “PLOT TO ATTACK ELECTRICAL SUBSTATION IN MARYLAND,” by anyone with a knowledge of the highest value “kill zone” in a substation, will take particularly serious warning that the alleged plot circumstances expressly demonstrate the sophisticated level of knowledge these alleged conspirators possessed, together with the capability

⁴ Video of the Sixth Meeting of the Joint Federal-State Task Force on Electric Transmission, available at the Federal Energy Regulatory Commission YouTube channel at <https://www.youtube.com/watch?v=bUTg2Rswdug> (accessed May 12, 2023)

to accomplish the goal of this plot which was to “...permanently completely lay this city to waste...” Baltimore, MD is the city these attackers sought to “lay waste to.”

While the above “conspiracy” was that of domestic extremists, it has been well documented for many years that foreign adversaries consider the electric grid to be our nation’s “Achilles heel” and thus a target for attack. Criminal cartels and foreign terrorist groups have successfully blacked out large portions of electric grids in other nations by means of physical sabotage. America’s porous border gives our foreign adversaries easy access to conduct sophisticated attacks against our own grid assets. Finally, the massive increase in “electrification” of everything from vehicles to cooking appliances and the rapid application of renewable energy assets to the grid are putting more stress on the grid than ever before. These factors must be a consideration when it comes to assessing the risks to these assets.

Discussion - New Metric for “Risk Assessment” is Needed

Regulators and Reliability Organizations, based upon a decade of review, conduct meetings and conferences in which physical security matters are considered. Attending to trade-offs involving losses and investments, the method they currently use to address physical security is known as the “Risk Assessment.” In simplified terms, the most commonly used metric focuses on the factors of “Frequency” and “Consequence” (or the equivalent). Based on the increasing frequency and sophistication of attacks against electric grid infrastructure, and the growing evidence that there is a persistent *intent* to conduct such attacks from domestic anarchist and extremist groups and foreign adversaries, a more prudent new metric is now required for these “Risk Assessments.” This new metric should incorporate real-world factors that pertain to the risks associated with physical sabotage. These factors include: (1) known vulnerabilities, (2) attacker capabilities, (3) and attacker intentions. “Frequency” is not a substitute for predictability in a prudent threat assessment and should not be conflated with the above factors.

Current FERC Dockets Pertaining to Physical Security Standard

On December 15, 2022, FERC filed an “Order Directing Report re North American Electric Reliability Corporation” under RD23-2-000. The order directed the North American Reliability Corporation to evaluate Reliability Standard CIP-014-3.

On February 15, 2023, in Docket No. AD21-15-000, the Joint Federal-State Task Force on Electric Transmission (Task Force) convened for a public meeting to discuss physical security of the transmission system.⁵

On April 14, 2023, in Docket No. RD23-2-001, the North American Electric Reliability Corporation (NERC) submitted its report (NERC REPORT) on its study evaluating Reliability Standard CIP-014-3, as directed by the Commission’s December 15, 2022 order.

That order was specified to evaluate (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard CIP-014-3 (Physical Security Reliability Standard); (2) the required risk assessment set forth in the Physical Security Reliability Standard; and (3) whether a minimum level of physical security protections should be required for all Bulk-Power System transmission stations and substations and primary control centers. That NERC Report is titled “Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System” and is included in this Petition as **Exhibit C**.

Applicability Under CIP-014-003

The NERC Report ⁶, and the discussions of the Sixth TASK Force Meeting indicated to Petitioner that an amendment is prudent and required, at this time, to enhance what is determined to be Critical Infrastructure under the Physical Security Standard CIP-014-003.

⁵ Ibid.

⁶ “Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System” <https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/NERC%20Report%20on%20CIP-014-3.pdf> (accessed May 12, 2023)

Applicability under CIP-014-001 is confined to what constitutes the BES, as declared in CIP-002.51a. Thus, we cannot seriously consider reformation or expansion of CIP-014-003 without first considering the electric assets that can, if damaged, permanently destroyed, or otherwise rendered inoperable, lead to uncontrolled separation, cascading outages or instability.

This engineering fact-of-life requires a review and new standard rule that would eliminate the exclusion of such electric assets that are considered as critical infrastructure by RTOs ISOs and Utility Companies, writ large, due to how these assets function in the system, and if not functioning, would cause the creation of uncontrolled separation, cascading outages or instability.

Petition for a FERC Order for an Enhanced Applicability Standard

The essential element of an operating electric power grid are the engineering models used ubiquitously in the U.S. electric grid system operation for planning, protections, monitoring load flows, and the interconnection of new transmission facilities.

As a career-length power engineer who has served with NERC Committees on the operations side of reliability has recently published an article titled: **“Plausible Deniability Rather Than Pragmatic Solutions the Signature of NERC CIP”**⁷ which states:

“Based on the current scope of CIP-002-5.1a and CIP-014-3 the grid will face large scale outages due to unrecognized critical facilities. Based on the NERC Report to FERC it appears these issues will remain unresolved.” ...

“It is important for the Commission and NERC to redefine the criteria of CIP-002-5.1a and CIP-014-3 by developing criteria for critical infrastructure that is defined by the RTO’s, ISO’s and utilities models which would provide a more accurate account of critical infrastructure.”

⁷ Michael Swearingen, “Plausible Deniability Rather Than Pragmatic Solutions the Signature of NERC CIP” <https://securethegrid.com/plausible-deniability-rather-than-pragmatic-solutions-the-signature-of-nerc-cip/> (accessed May 12, 2-23)

“This would provide the Commission and NERC with already established engineering models that could be available for review upon request in any timeline they would consider prudent. However as stated in their report, they are not recommending “an expansion of the CIP-014 Applicability criteria at this time”. It seems with all the content contained in the 31-page report submitted by NERC the main takeaway would be that NERC is open to tabletop discussions of potential measures but is currently satisfied with the status quo”.

This report, as it stands, is concerning as it continues to allow a vacuum in security that exists through the scope and exclusionary method of standards as currently enforced. Should this trend continue concerning electric grid security and the stress on the grid growing due to the aggressive expansion of green energy without comparable expansion in grid facilities, the nation will be facing a less reliable electric grid and more large-scale outages more frequently.”

[This article is attached as **Exhibit D**]

It is apparent from engineer’s perspective that the industry operating models enable the utilities to know precisely which elements of their grid equipment are most critical and that these models are not being used to consider which facilities ought to be better protected against physical attack.

We therefore petition the Commission to order an enhanced applicability standard that would:

- (1) Require the regional authorities to use these amalgamated operating models to designate the critical assets that ensure the reliable flow of power, and lessen the risk of uncontrolled separation, instability, or cascading outages.
- (2) Require the industry to establish new metrics for Risk Assessments that incorporate real-world factors pertaining to the risks associated with physical sabotage, such as known asset vulnerabilities, attacker capabilities, and attacker intentions. [One known “asset

vulnerability” should be whether an applicable asset (such as a large power transformer) is vulnerable to ballistic attack and currently unprotected against such an attack.]

Conclusion

We believe that FERC must demand that the utility industry use their own engineering operating models to re-assess which assets are “critical” and that they overhaul their “risk assessment” process to comport with real world threats and the real and present vulnerabilities of those assets. History demonstrates that the industry will not take these steps on their own, underscoring the importance of urgent FERC action on this matter.

Respectfully submitted,



Thomas J. Waller Jr.
Co-Director
Secure-the-Grid Coalition
twaller@centerforsecuritypolicy.org



Douglas Ellsworth
Co-Director
Secure-the-Grid Coalition
doug.ellsworth@usapact.org

1 UNITED STATES OF AMERICA

2 FEDERAL ENERGY REGULATORY COMMISSION

3

4 Sixth Meeting of the Joint Federal-State Task Force

5 on Electric Transmission

6 Docket No. AD21-15-000

7 TASK FORCE CONFERENCE, IN PERSON AT THE WASHINGTON

8 RENAISSANCE HOTEL IN WASHINGTON, D.C., AND ONLINE VIA ZOOM

9 Federal Energy Regulatory Commission

10 888 First Street, N.E.

11 Washington, DC 20426

12 Wednesday, February 15, 2023

13 1:30 - 4:00 p.m. EST

14

15 Dr. Jonathan Raab (Moderator)

16

17 FERC Commissioners

18 Chairman Willie Phillips, Commissioner James Danly,

19 Commissioner Allison Clements, Commissioner Mark Christie,

20

21 Staff:

22 General Counsel, Matthew Christiansen

23

24

25

1 State Members

2 Mid-Atlantic Conference of Regulatory Utilities

3 Commissioners:

4 Chair Gladys Brown Dutrieuille, Pennsylvania Public Utility

5 Commission

6 Chair Jason Stanek, Maryland Public Service Commission

7

8 Mid-America Regulatory Conference:

9 Chair Andrew French, Kansas Corporation Commission

10 Chair Dan Scripps, Michigan Public Service Commission

11

12 New England Conference of Public Utilities Commissioners:

13 Commissioner Riley Allen, Vermont Public Utility Commission

14

15

16 Chair Marissa Paslick Gillett, Connecticut Public Utilities

17 Regulatory Authority

18

19 Southeastern Association of Regulatory Utility

20 Commissioners:

21 Commissioner Kimberly Duffley, North Carolina Utilities

22 Commission

23 Chair Tricia Pridemore, Georgia Public Utilities Commission

24

25

1 Western Conference of Public Service Commissioners:
2 Commissioner Darcie L. Houck, California Public Utilities
3 Commission
4 Chair Ted LeVar, Utah Public Service Commission

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 P R O C E E D I N G S

2 1:30 p.m.

3 MR. CHRISTIANSEN: Good afternoon everyone. My
4 name is Matthew Christiansen. I'm FERC's General Counsel,
5 and this is the time and place that has been noticed for the
6 Sixth Meeting of the Joint Federal-State Task Force on
7 electric transmission to consider the matters that have been
8 posted in the agenda issued on February 1, 2023, in Docket
9 AD21-15.

10 This meeting is on the record, and a transcript
11 will be placed into the docket. The public can listen and
12 observe in the room and online. Any comments by the public
13 can be submitted into the docket through FERC's e-filing
14 system. Please visit FERC's website for more detail.

15 Today's discussion will avoid the merits of any
16 pending contested matter, and I will interrupt discussions
17 if we enter that territory. Task Force members can address
18 matters raised in pending proceedings generally, but should
19 not speak to the specific merits of a pending, contested
20 proceeding. With that I'll turn the Task Force over to FERC
21 Chairman Willie Phillips, and Maryland Public Service
22 Commission Chair Jason Stanek. Thank you.

23 CHAIRMAN PHILLIPS: Thank you Matt, and welcome
24 everybody to the sixth Task Force meeting. Before we begin
25 I want to just take a moment and thank former Chair Glick

1 for actually establishing this Task Force. I can tell you
2 as a former state regulator, and on behalf of my state
3 colleagues, having your voice heard in a meaningful way
4 makes a big difference, and so I thank Chair Glick.

5 I also want to take a moment to recognize former
6 Massachusetts Chair Nelson, who we know was an active
7 participant in this Task Force. He will be missed. Before
8 I turn it over to Chair Stanek for his opening comments, I
9 do want to just say a little bit about today's topic. I
10 think today's topic is very timely. I don't have to tell
11 you all. We've seen it in the news as of late.

12 Recently, we've seen several incidents. The U.S.
13 power grid was physically attacked 107 times in the first
14 eight months of 2022. Reports of substation ballistic
15 incidents increased more drastically in 2022, than the
16 overall increase in ballistic incidents. And these events
17 correspond with an increased extremism in our country.

18 According to a study by George Washington
19 University in 2016 to 2022 white supremacists' plots
20 targeting energy systems "dramatically increased in
21 frequency." So as regulators the reliability and resilience
22 of our bulk power system and our local distribution systems,
23 it is paramount. We know this.

24 And so in December we asked NERC to take a
25 careful look at our CIP 14 physical security reliability

1 standards. That report is due out in April. And also, it
2 was at the beginning of this year when I was named Chair,
3 and I spoke with Chairman Stanek and we decided that we
4 would love to invite NERC CEO Jim Robb, and Director Kumar
5 from DOE to come and talk a little bit, and help educate
6 both FERC and the state commissions on this very important
7 topic. So with that I'll turn it over to Chair Stanek.

8 CHAIR STANEK: Thank you Chair Phillips, and
9 welcome everybody to our sixth meeting. Let me just begin
10 by stating on behalf of the ten state Commissioners here,
11 congratulations on your elevation to FERC Chair. We
12 appreciate seeing one of our own, somebody who has been in
13 the State Commissioner's shoes, understands the challenges
14 that we face, particularly on these issues relating to
15 transmission, so congratulations.

16 Yesterday at the electricity committee meeting
17 you were recognized, and this was really important to us
18 that your first act in office was to ensure that there was
19 continuity between you and Chair Glick in having this Task
20 Force continue part of the charge, the three year charge, so
21 thank you.

22 I'd like to also echo my thanks to Chair Glick on
23 behalf of the State Commissioners for green lighting this
24 concept which was never formally invoked under FPA 209 to
25 have this joint board serve for the period of three years.

1 It's been productive over the past two years, and we look
2 forward to continuing the conversations into the next year.

3 I would also like to thank Chair Matt Nelson, who
4 has served so valiantly over the past two years with him and
5 his staff making very significant contributions to a lot of
6 the filings and comments that were submitted by NARUC. So
7 as Chair Phillips just alluded to, the format is going to be
8 a little different today, as opposed to responding to NOPRs
9 and ANOPRs, and other concepts that were placed on the table
10 by our FERC colleagues.

11 Today's mission is more of a fact-finding, and
12 we're honored to have two esteemed guests from NERC and DOE
13 with us today to share their insights. Over the past eight
14 weeks the State Commissioners have had half a dozen
15 classified meetings with various members of industry, better
16 understanding the physical threats that affect our local
17 distribution grids.

18 Finally in my backyard yesterday we had the
19 indictments of two very concerning individuals who planned
20 five coordinated attacks at the Baltimore Gas and Electric
21 substations. If you read the criminal complaint, which is
22 in the public domain, it reads like a Hollywood story
23 involving robberies of convenient stores with machetes, two
24 murders of the fellow's roommates, and then the plot on
25 these five substations with the intent to "level and

1 totally destroy the City of Baltimore."

2 These were Neo-Nazis as the Chair just alluded
3 to. But the level of planning, reviewing the transcript,
4 you would think that these were two transmission operators.
5 Oh no, we have to take out the fifth line, not the fourth
6 line. We need to use high caliber artillery to get to the
7 core of the substations. We have new threats.

8 We need to stay one step ahead, and I think this
9 conversation today will not only further develop the
10 relationships between the state and federal counterparts,
11 but further techniques that will keep us one step ahead of
12 these criminals that seek to wreak destruction on the
13 distribution and transmission systems.

14 So I'm looking forward to the comments today.
15 I'd also like to recognize that we have one new addition to
16 the virtual table today, and that is Chair Marissa Gillett
17 of the State of Connecticut. And one thing I'm very proud
18 about Marissa is that before she went to Connecticut to
19 assume the Chairmanship, she was a staff member at the
20 Maryland Public Service Commission in Baltimore.

21 So we look forward to having her, and I turn to
22 her for some opening introductory comments.

23 CHAIR GILLET: Thank you so much Chair Stanek. I
24 am so sorry for my first meeting that I am not able to join
25 in person, as I know many of you can relate to. It's a busy

1 time of year for us with the rate case evidentiary hearing
2 starting tomorrow, as well as a draft decision in another
3 rate case due the same day, so I regrettably had to stay
4 behind for this meeting. I look forward to joining you in
5 person at future meetings.

6 I too echo the same, for Chair Nelson's service
7 on this preceding me. I tried to pick his brain, along
8 with Commissioner Riley Allen, to figure out where he left
9 off, so I can pick back up. I look forward to bringing to
10 the conversation a similar perspective that you have gleaned
11 from Chair Nelson. I think the southern portion of New
12 England has many challenges, just as each of your all's
13 regions do, and I look forward to bringing that same kind of
14 energy and perspective to these conversations.

15 So thank you so much for the invitation to
16 participate on this important Task Force. I echo the
17 comments from Chair Stanek regarding the importance of
18 having conversations between state and federal regulators,
19 and I'll look forward to the conversation, so I'll turn it
20 back to you. Thank you so much.

21 DR. RAAB: Welcome everybody. Just a few quick
22 of our ground rules, or way of moving together here, and
23 then we'll jump right into the substance. Just a quick
24 reminder we've got two State Commissioners from each region.
25 Just be clear when you're giving your own personal

1 perspective, or your own state perspective, otherwise we're
2 assuming you're kind of thinking about your region as a
3 whole.

4 Second, if you want to speak, it's the
5 old-fashioned just -- and Marissa I have your card here, if
6 you want to speak just raise it up and I'll keep the queue.
7 And third, just speak pretty closely to the mic, so
8 everybody can catch every word of your wisdom here.

9 We have two parts today if you will. The first
10 part, which is new to the Task Force to have some guest
11 presenters, and as the Chair said just looking at this kind
12 of as a joint fact-finding. I think for this, everybody is
13 still learning. And then the second half after we say
14 goodbye to our guests, we'll go more a little bit into the
15 old-fashioned Task Force of really trying to think through
16 what things might be useful to make improvements in this at
17 both the state and federal levels.

18 So the way that we've got the next hour set up
19 I've asked President Robb, not Raab, Robb, and Director
20 Kumar to each give just a five minute intro of some main
21 points that they want to make. And then we have a series of
22 questions that we worked together collectively, the Task
23 Force bouncing back and forth on things that they wanted to
24 ask you.

25 And so I will ask those questions. They've seen

1 the questions before. We'll have each of them talk for just
2 a minute or two in response to the questions, and then we
3 want to have a discussion with the time that we have with
4 the Task Force members, so before we move on from a
5 question, or in some cases two questions together, we'll ask
6 you for any follow on questions.

7 If you want to make some points, a little more
8 free flowing with the timeframe that we have. So without
9 further ado we'll turn first to Jim.

10 PRESIDENT ROBB: Thank you, Jonathan. I like the
11 sound of that President Robb thing. I've never heard that
12 before. I have to start by acknowledging that the last time
13 I was in an open session with Chairman Phillips there was a
14 little bit of trash talking going back and forth between
15 then number one, Purdue Boilermakers, and then number three,
16 Alabama Crimson Tide.

17 I have to eat crow and acknowledge that the
18 Boilers have since lost a couple games. We're now number
19 three, not number one, so congratulations Mr. Chairman. So
20 first of all, thank you very much for the opportunity to
21 share some thinking with you, and perspectives on physical
22 security. It's clearly a very timely, and a very important
23 conversation, so I appreciate it.

24 It's also a very tricky conversation,
25 particularly in a setting like this, so we'll do our best to

1 be as disclosive as we can, but understanding the nature of
2 this we may be a little guarded on a few things. It's
3 abundantly clear as the Co-Chairs opened with that over the
4 last decade or so, our society has become increasingly
5 dependent on electricity, and an uninterrupted supply of
6 electricity.

7 And that's, you know, a big part of the mission
8 of NERC, and a big part of the mission of the states, and
9 electricity now affects every portion of our lives, so it's
10 something that we need to take very, very seriously.

11 It's also important to note that the
12 infrastructure that supports that uninterrupted supply of
13 electricity is widely disbursed, largely above ground, and
14 it creates all sorts of physical vulnerabilities, not just
15 to acts of sabotage, which is the principal topic of today,
16 but also you know, protection against the increasingly
17 extreme weather events that we're seeing around the world
18 these days.

19 As you probably know, there are well over 50,000
20 high voltage substations across North America, and more than
21 that if you include those that only support the distribution
22 system. That's a tremendous amount of infrastructure to
23 think through how to protect responsibly, and to really
24 think through the trade-offs that need to be made between
25 risk and consequence, and the investments that you make

1 between protection and prevention, versus response and
2 recovery.

3 And it's very important as we kind of enter this
4 conversation that we always keep in mind those trade-offs
5 because it's not a simple as we should just protect
6 everything because your rate payers, that you're responsible
7 for it, probably wouldn't like that answer.

8 So we need to be very thoughtful about how we
9 approach this whole conversation. So without going into all
10 the details right, it's clear that there are a number of
11 natural hazards that the system needs to be hardened
12 against, but physical attacks on electric infrastructure as
13 reported to the E-ISAC have definitely increased over the
14 last couple years, and are resulting in impacts of greater
15 consequence.

16 You know, typically and historically, we've
17 always seen a high level of activity, which we would, you
18 know, describe as criminal mischief -- break-ins, intent to
19 steal copper to sell on the black market and the like, but
20 over the last six to nine months we've seen more and more
21 attacks, which would exceed the threshold of criminal
22 mischief, and really rise to the level of sabotage.

23 And clearly, the events in Moore County, the
24 Seattle Tacoma attacks, which resulted in outages last
25 December, and the plot that was recently announced that the

1 FBI thwarted in Baltimore has triggered significant concern
2 around the physical security of our electric infrastructure,
3 and the protections against it, and I think that's highly
4 appropriate.

5 I think one statistic that's important to keep in
6 mind is that the vast majority of physical security events
7 as we understand them do not result in any impact to the
8 grid, only less than 5 percent have resulted in any grid
9 impact. And by grid impact I mean either a loss of the
10 ability of the grid to perform, to serve customers, damage
11 to equipment, or something that would put the grid into a
12 contingency operation mode.

13 That's relatively good news. But the bad news is
14 that I've said these attacks are happening more quickly, or
15 more frequently. Extremist groups post instructions for
16 disrupting critical infrastructure on the dark web, and
17 they're increasingly acting in emboldened ways, and
18 potentially in coordinated ways as we've seen with this
19 Baltimore event.

20 So it's clearly an issue that the electricity
21 ecosystem, and when I say ecosystem I want to bring into
22 that law enforcement, clearly needs to be focused and come
23 together around. Another bit of reassuring news here, the
24 electric system, despite its sprawling above ground
25 topology, has built into it an extraordinary level of

1 redundancy, which in and of itself creates resilience.

2 You know, from a NERC perspective it's probably
3 important to keep in mind that we are primarily concerned
4 with the protection of the bulk power system, you know,
5 which we typically think of as transmission above 100 kV,
6 generation of above 75 megawatts, as the bulk system.

7 And our focus is all around preventing what we
8 colloquially will call the evil three, which is an
9 uncontrolled separation, cascading outages or instability.
10 That's the framework and the mindset from which CIP 14,
11 which is our physical security standard was born.

12 CIP 14 recognizes that, and it's structure in
13 such a way that only those assets that could create a major
14 cascading event, are required to have necessary physical
15 protections put in place. The standard requires most
16 substations above 345 kV to have a risk assessment
17 performed, validated by an independent third party, and then
18 appropriate protections put in place, based on the hazards
19 that that substation needs to defend against, and that also
20 needs to be validated by an expert third party.

21 It's designed to give great flexibility to
22 utilities as to how to comply, since each critical asset may
23 have unique risks that will require unique mitigation, so
24 it's prescriptive on process, not prescriptive on
25 mitigation. And the consequence we're protecting against,

1 again it's important to remember, is the cascading event
2 that would affect millions of customers, not thousands.

3 The last bit of the reassuring news I'll share is
4 that CIP 14 sets a minimum threshold for a risk assessment
5 and protection, and it's a baseline. And as with many of
6 our standards, industry doesn't stop there, and it will
7 typically go well beyond what the standards call for. So
8 while many substations may not need to be technically CIP 14
9 compliant, their owners may very well build in protections
10 because it's the right thing to do.

11 The utility sector generally leans in very, very
12 hard on security matters, whether physical or cyber, to
13 protect their assets and their ability to serve their
14 customers. CEO engagement at the ESCC, the Electricity
15 Subsector Coordinating Council, and the investment that we
16 have made in strengthening the capabilities of the E-ISAC,
17 and the very fluid relationships between us, industry and
18 our government partners such as DOE, really reflects that
19 commitment.

20 And I think the efforts that Puesh has undertaken
21 over the last year to set up, stand up what we call the
22 Energy Threat Analysis Center, a very novel way for the
23 private sector and public sector, you know, to come
24 together, look at raw intelligence, and enrich it with
25 purpose relative to the sectoral needs. I think really

1 reflects the attitude of the industry to lean into these
2 issues.

3 And I think as I wrap up here, and before I hand
4 it off to Puesh, I wanted to just kind of summarize three or
5 four of the things that we're thinking about as we conduct
6 this assessment that FERC directed us to do on physical
7 security and CIP 14. I think one question that's clear on
8 the table has to be whether or not the risk assessments
9 should continue to focus only on the loss of a single asset,
10 an N minus 1 condition, or should we look at the situations
11 where more than one asset is taken out? "The coordinated
12 attack."

13 You know, that's kind of what we saw happen in
14 Baltimore, as we understand it, and a bit of a situation we
15 had in North Carolina. So the question is should it still
16 be a single contingency, or should we look at multiple
17 contingencies from a risk assessment?

18 Second, should the risk assessment be focused
19 primarily on the prevention of a major cascading outage, or
20 should we somehow figure out how to incorporate
21 appropriately the concept of customers impacted, given
22 society's growing dependence on electricity?

23 Third, right, how should the mitigation plans
24 best optimize between investment and protective measures,
25 versus investment in the ability to arrest and restore and

1 recover from an event. And then finally, I guess this is a
2 very appropriate thing for this audience, is there a way
3 through our standards to create the framework for a more
4 direct dialogue between the utilities and the state
5 regulators who will have to approve cost recovery for any
6 investments that are made around the risks that's embedded
7 in their systems, the costs to mitigate that risk, versus
8 the cost to recover, and have a collaborative conversation
9 around how much risk are you willing to wear, versus how
10 much do we want to mitigate.

11 And when we mitigate, do we want to do that
12 through prevention or recovery? I think those are the
13 questions that we'll be focusing a lot of our time and
14 attention on. And so with that, Puesh I'll hand it off to
15 you.

16 DIRECTOR KUMAR: Great. Thanks so much Jim, and
17 good afternoon everyone. I'm Puesh Kumar. I'm the Director
18 of DOE's Office of Cybersecurity, Energy Security and
19 Emergency Response or CESER, and thank you to the Joint Task
20 Force for hosting this important conversation.

21 This is a topic certainly that's been top of mind
22 for us at the Department, and we certainly have received a
23 lot of inquiries from a lot of different people on this
24 topic, and so it's timely, it's a good conversation that we
25 need to be having, not only with our federal partners, which

1 we've had a tremendous relationship with our colleagues at
2 FERC, and of course, the leadership of Jim, and the NERC,
3 and the electricity ISAC has been great, but it is a
4 conversation of the state level as well because when these
5 incidents happen you immediately get calls to Governor's
6 offices.

7 You get calls to PUCs in terms of what's
8 happening, and what more do we need to be doing. And so
9 this is something that is again, a timely topic, so I look
10 forward to the discussion. I'll say upfront I may not have
11 all of the answers, and I would like to hear some of the
12 thoughts from some of the Commissioners at the state level
13 in particular, on what are solutions to address some of
14 these challenges.

15 I'll certainly offer ideas we have from our end,
16 and things we could be doing jointly, along with Jim and
17 others, but would also welcome hearing thoughts from our
18 colleagues on the state side. You know, the reality with
19 these incidents, you know, one thing we take a step back and
20 take a look at incidents like the Metcalf substations, or
21 the one in Moore County, or the one in Tacoma.

22 The first thing, there's a couple pieces here
23 that I want to acknowledge upfront, and one while Metcalf
24 didn't actually result in power outages, it was a very
25 significant incident. It was a paradigm shift for us, which

1 is what resulted in the development of CIP 14. That was ten
2 years ago.

3 So that's one datapoint. The second datapoint is
4 in the case of Moore County, that one resulted in an impact
5 of 40,000 customers being without power during a time when
6 it was in the winter weather, and while it did not impact
7 the bulk power system, it did have an impact on the delivery
8 of power to Americans across the country, and that should be
9 concerning to all of us.

10 Now what are the solutions to this? And that's
11 the harder question that we're hopefully here to explore.
12 And then the last piece of this, I know I don't have our law
13 enforcement colleagues in the room today, but I just want to
14 reiterate the fact that this is something that they too are
15 very focused on, and we're happy -- I'm happy to get into
16 some of the conversations that we have regular meetings with
17 our colleagues at the FBI, at the Department of Justice, and
18 the broader inner agencies.

19 This is a concern to everybody, and so I was
20 really glad to see the efforts of the FBI to disrupt the
21 plot targeted at Exelon and Baltimore Gas and Electric. And
22 I think this is when we think of the law enforcement angle,
23 that again doesn't need to just be at the FBI level. We
24 need to make sure that we have local law enforcement, we
25 have state law enforcement also engaged in this

1 conversation, and really recognizing, and appreciating the
2 criticality of the electricity infrastructure across the
3 country.

4 Again, there are over 75,000 substations, 69 kV
5 and above, we need everybody really focused on this problem,
6 and we need to be attacking it from all angles, and that's
7 the approach we want to take at the Department of Energy.
8 Now I would like to take a step back, and one of the things
9 we do in CESER is we look at risks from an all hazards
10 perspective.

11 When we think of security and resilience we have
12 to look at the fact that it's not a single physical
13 security. Physical security isn't the only thing that we
14 are being challenged by, we're also being challenged by
15 increasing cyberthreats. We're also being challenged by the
16 increasing climate based risks across the country.

17 And so if we look at this multi-threat
18 environment, how do we ensure that we build standards,
19 policies, and tools and technologies that really try to buy
20 down risk broadly. So if there's a measure we're taking in
21 place to protect substations from a physical security
22 perspective, can we have an added benefit from a
23 climate-based risk perspective? We really do need to be
24 thinking about how all of these risks we're facing, all
25 these risks are upon us, and what do we need to do more

1 broadly as we invest in the security and resilience of the
2 grid going forward?

3 A big focus area for my office is preparedness.
4 We need to prepare for the majority of the time, and then
5 during an incident we need to respond to these types of
6 incidents. Now that preparedness comes in a lot of
7 different ways. One is policies. And we need to constantly
8 be thinking about how the risk is changing, and how should
9 that inform both federal policies and state policies to keep
10 pace with the evolving risk?

11 We also look at capacity building and training.
12 How do we work with owners and operators in partnership with
13 NERC and the E-ISAC to ensure they have the latest
14 information, whether it's threat information, or whether it
15 is other training and resources to harden infrastructure in
16 light of the changing risks that we're seeing.

17 And then last but not least, how are we investing
18 in tools and technologies that could also help us buy down
19 the risk. You know, what we always think about is it's not
20 just the standard that buys down risk, there's a lot of other
21 ways, and tools and technology is part of the puzzle that we
22 have to be thinking about that could certainly help along
23 those lines.

24 I was on a panel earlier at NARUC talking about
25 that, and our colleagues from PPL also had ideas of how

1 they're thinking about using technologies to again reduce
2 risk. So we really do need to think about it more broadly.
3 Now specifically, about the physical security environment
4 that we're in, the Department of Energy, much like NERC,
5 through their EOP process, gets reports of incidents, all
6 types of incidents, that could affect the bulk power system.

7 And we have seen an increase in physical security
8 incidents since this past year alone. And that is a fact
9 that we have to acknowledge, that we've seen more physical
10 security incidents. Now what types of incidents are we
11 seeing? The majority of the incidents that we've seen have
12 been vandalism. They have been theft, copper theft that
13 we've seen for a long time in this sector, but of course,
14 the more concerning ones have been some of the targeted
15 gunfire that we've seen.

16 And so when we look at the entire list of
17 incidents it does still -- the majority of them are still
18 focused on petty theft and vandalism across the sector. So
19 you really when you look at risk characterization, that's an
20 important fact as we think about what measures we need to
21 buy down those types of threats, because then that helps us
22 build in better protections going forward.

23 And then on the law enforcement front, we're
24 continuing to stay engaged with our colleagues at FBI, and
25 we actually worked with FBI recently to provide a briefing

1 to folks across the field offices across the country, in
2 terms of understanding the criticality of infrastructure so
3 that where there is reporting of this type of an incident by
4 a utility, we can make sure we're connecting dots quickly,
5 we're getting information out to the broader sector through
6 mechanisms such as the ISAC, that everyone can understand
7 what happened, and how do we better protect those systems
8 going forward?

9 And so I do again want to commend our colleagues
10 at the FBI. Now Jim, you hit on a really important piece,
11 which is risk versus cost. The reality is there is always
12 going to be more work we need to do. Our work will never be
13 finished in this space because the risks continue to outpace
14 everything we're doing. It continues to shift and change,
15 and the reality is as we see the grid evolve, as we see new
16 tools, technologies, come into the grid we're going to see
17 significant investment in the grid over the next five to ten
18 years.

19 We have to think of strategies to ensure the
20 security and resilience of not only the infrastructure of
21 today, but the infrastructure of tomorrow. Now the
22 infrastructure of tomorrow could also be an opportunity we
23 have to build in security and resilience, and harden the
24 infrastructure. So we need to be keeping that in mind as we
25 think about solutions.

1 It can't just be thinking about the solutions we
2 have today, but it's the solutions that could be brought by
3 this evolving grid dynamics that we're going to see going
4 into the future. For example, the 62 billion dollars that
5 the Department of Energy is going to be investing, the 369
6 billion dollars of Inflation Reduction Act, through both
7 loan guarantees and direct investments.

8 And then what on average has been cited as about
9 100 billion dollars in private investments over the decade
10 every year. So tons of investments are going to be
11 happening, and we have the opportunity now to ensure the
12 security and resilience. I'll wrap up there because I know
13 we have a lot of really good questions prepared, but I
14 appreciate the time. Thank you for involving us in the
15 conversation.

16 DR. RAAB: So we're going to just systematically
17 work through a set of issues and questions. You've both
18 touched on many of these. It will give you a chance to go
19 into a little bit more depth, and also a chance for the Task
20 Force to ask follow-on questions, and also weigh in.

21 So the first two topics we'll do together. One
22 is on the types of threats, and one is on the impacts of
23 physical attacks. I'm just going to read the questions just
24 so the audience is sort of in sync with what we're doing.

25 So the first on the first of types of threats,

1 what are the main types of threats and vulnerabilities to
2 the physical security of the transmission system, and how,
3 if at all, do they differ regionally, like based on load
4 density and geographic features, and how are these sets of
5 vulnerabilities evolving?

6 And then secondly, what can be the impacts of the
7 attacks on the reliability of the transmission system? And
8 are these impacts typically limited to a single transmission
9 owner's footprint, or more regional in nature? And Jim
10 you're going to go first with a couple minutes.

11 PRESIDENT ROBB: Sure. So I touched on some of
12 this, and so did Pugh in our opening. Typically we've seen
13 vandalism, break-ins, you know, geared around theft, and so
14 forth. It's really been over the last several years. I
15 mean there's always been kind of like we could always refer
16 to them as the drunk hunters, right, that will go out and
17 will fire at electric equipment.

18 But what we've seen over the last several years
19 clearly there's been an increase in ballistic activity, and
20 in step with clearly intent to harm equipment as opposed to
21 whatever else might motivate someone to do this work. One
22 thing I do want to underscore is it's very rare that we get
23 a -- we find out who did it, and we have an incarceration so
24 that we really know what motives are, right?

25 So a lot of our understanding of motivation is

1 speculative. And it's important to understand that as well.
2 I don't think we've seen a real variance across regions, but
3 we have seen clusters. There's been a cluster of activity
4 in the Pacific Northwest. There have been clusters of
5 activities in the Carolinas and in the south, and then in
6 kind of around Texas, Oklahoma, Arkansas area, are three
7 that come to mind.

8 So we are seeing some repeat events, and some
9 clustered events, particularly over the last several years.
10 I think in terms of the impact on the system for the most
11 part there's almost none. You know, it takes an awful lot
12 to damage equipment to the point where it can't function.

13 That is what we saw though in North Carolina. We
14 saw that in Seattle, Tacoma, and we almost certainly would
15 have seen that in Baltimore had these characters been able
16 to carry out the plans that they had.

17 So typically, there's no service impact. And if
18 there is it's typically something that the utility can
19 dispatch around. That was the situation with the Metcalf
20 substation outside of San Francisco. Even though it was a
21 very paradigm changing attack, it didn't really result in
22 any electric impacts. So it's been fairly rare, and really
23 just recent that we've seen outages of the scale that we saw
24 in North Carolina, or in Seattle Tacoma around these
25 events.

1 As I said, I think the thing that we need to chew
2 on collectively is, you know, is the loss of a single
3 element of the system the right test? Or do we need to be
4 thinking more about multiple elements given this observation
5 that we have at least one bona fide coordinated attack being
6 planned, which is the one in Baltimore.

7 I don't know all the specifics around Moore
8 County, to know how much insight the individuals there had
9 into the grid that they were attacking, and even less in the
10 Seattle Tacoma area. So there's more insight to be gained
11 out of those events, but I think the question around defense
12 against coordinated attack has to be something that's on the
13 table.

14 DIRECTOR KUMAR: I'll just add a little bit more.
15 Jim covered it well. Just to give you a little bit of data
16 in terms of the filings to the Department of Energy in terms
17 of the types of incidents we've seen related to physical
18 security. So in 2022, there were 390 DOE 417 reports filed
19 with the Department of Energy in terms of all incidents.
20 That is everything from cyber to physical, to even things
21 like an animal causing an outage.

22 It really does span the entire gamut of anything
23 that could disrupt the bulk power system. We want awareness
24 of what's going on, so we can respond to it, and prepare for
25 it if need be. Now specifically, of that number, there were

1 163 events that were categorized as physical, and that
2 includes vandalism, suspicious activity, sabotage, it really
3 does range across the board, and just more broad.

4 Now, of those 163, 80 were vandalism, so just to
5 give you a picture. Now how does that compare to 2021? So
6 in 2021, there were a total of 92 reports that were physical
7 in nature in some way or another, again vandalism, theft, or
8 some type of physical incident. And then in 2022 it was
9 163. So again there was an increase, and so we have to be
10 watching what is happening, what's causing that.

11 Now the majority of the incidents as Jim
12 mentioned, there isn't a lot of good information on what
13 caused it, and this is where I know our colleagues at the
14 FBI and others would like to have better fidelity on what's
15 going on, so that they can also do what they do best, which
16 is connect different dots and figure out what's going on.

17 But in most cases we don't know. Now in some of
18 the cases we do, and that's where things like the Exelon,
19 BG&E disruption was able to happen because FBI was able to
20 better understand what happened there, and get ahead of it,
21 and that's good. So just wanted to put some data out there
22 in terms of what numbers of reporting we've received in this
23 space.

24 DR. RAAB: Before we leave these two topics, any
25 follow-on questions or points that Task Force Members want

1 to make? Commissioner French?

2 COMMISSIONER FRENCH: Just a question for Mr.
3 Robb. I think, you know, we've talked about the fact that
4 one of the great strengths of our electric grid, unlike some
5 others in the world, is we're very decentralized. We have a
6 very meshed AC system, largely looped, not too radial.

7 And so, when these events do occur, they tend to
8 be pretty localized, you know, I hesitate to say, but sort
9 of blips on the local system usually. I think that's what
10 you just alluded to, that you know, we've not seen big
11 outages. And I agree with all of that. But I'm struck by
12 you have this other comment of do we need to start looking
13 at multiple event scenarios N of 2, N of 3, N of 4 and so
14 on, and so I wonder have you given any thought to what the
15 right strategy, or the least cost strategy may be to address
16 those situations whether it is physical hardening of every
17 facility, or is it even further decentralization of the
18 grid, more redundancy of the grid as a least cost option?

19 PRESIDENT ROBB: Commissioner that's a great
20 question, and at the heart of that is a very important
21 insight that we saw when CIP 14 was being developed and put
22 in place. The best way not to create compliance risk around
23 a standard is not having any of those assets in your system.

24

25 So you know, the more that as we redevelop

1 systems, you know, around either a new generation mix, or a
2 storm recovery, any of those kinds of events that cause the
3 system to be reconfigured, the more we can reduce our
4 dependence on any of these, what we currently think of as
5 critical substations is God's work, right?

6 As it turns out I actually do not know the number
7 of how many critical substations have been identified
8 through the CIP 14 process, nor do I really want to know
9 that number. But it's certainly a very small number, and I
10 think that's good. And I would love to see that number
11 continue to decline as we can build more and more redundancy
12 into the system, and less dependence on a subset of the
13 assets around the grid.

14 In terms of the right strategy I think you've got
15 to give us time to kind of complete the study because my
16 instinct tells me that hardening every facility in the
17 country against physical attack is not the winning
18 strategy. I think it's not affordable, and it would be an
19 inefficient use of resources. Other things that could be
20 very helpful though: standardization of equipment designs
21 right, that would allow you to share inventory, again to
22 promote very quick recovery from an event.

23 Very important. That's one of the issues that's
24 vexing the industry right now with all the supply chain
25 challenges that we have, a lot of this equipment isn't

1 standardized, so I think that's an opportunity as we move
2 forward. But I think, again as I said, the vast majority of
3 all the impacts that we've seen, even those that we
4 characterize as grid impacts have been highly localized,
5 and may or may not have even resulted in any outages at
6 all.

7 So again, I think you have to weigh the customer
8 impact of this -- perspective customer impact of this
9 relative to your cost to defend against it.

10 DR. RAAB: Other questions? I'm going to move on
11 because I know we want to hit everything while we have you
12 here. So you mentioned before that we have a required
13 process, but not necessarily required standards. And the
14 next question goes about requirements.

15 So what requirements, including mandatory
16 reliability standards are in place today regarding the
17 physical security of the transmission system?

18 PRESIDENT ROBB: Yeah. Just to give a review
19 very quickly how CIP 14 is constructed. First, we did a
20 high level risk assessment across the entire system, and
21 concluded that substations of certain characteristics
22 needed, or had the potential to be a consequential event if
23 they were taken out of line.

24 For the most part these are substations above 345
25 kV. It's not all 345 kV substations, but probably 90

1 percent of them qualify. It depends on the voltage, and the
2 number of lines that come into the substation that creates
3 the vulnerability, and the engineers figured out a formula
4 for doing that.

5 But the basic notion of the standard is to do the
6 risk assessment as to what the consequences would be if that
7 asset were taken out of service, and have that risk
8 assessment validated by a third party, and also what
9 vulnerabilities that substation has. Now obviously a
10 substation in a very rural part of the country will have a
11 very different set of vulnerabilities than one in downtown
12 Manhattan, right? So it's got to be done sensitively to the
13 physical structure that's built and the geography that it's
14 serving.

15 And then the utility is required to put together
16 a mitigation plan, to mitigate those risks, and again to
17 have that validated by an independent expert third party.
18 So one of the things we were trying to do with this standard
19 was to one, be very risk focused because not every
20 substation looks the same.

21 The consequence of an outage at every substation
22 is not the same, and the risks that any substation has, and
23 the proper way to mitigate those risks may be very, very
24 different. So we wanted to give maximum flexibility to
25 comply in a way that made sense for the characteristics of

1 that asset, but also to have this independent expert
2 validation right, so that we had comfort that the work was
3 done with integrity, and the mitigations that were put in
4 place would actually address the vulnerabilities that were
5 discovered.

6 DR. RAAB: So questions, or even observations
7 from the other Task Force members on this point because
8 we'll be returning to this later in our discussion? Chair
9 Scripps and then Commissioner Christie.

10 CHAIR SCRIPPS: Thanks. I appreciate that, and I
11 think that flexibility of the CIP standards is certainly one
12 of its strengths, and that it's sort of specific to the
13 individual risks that are uncovered. But I guess I'm still
14 not entirely convinced that there are no measures that
15 should be included as sort of a baseline, and I say it for
16 two reasons, and would love to get your response.

17 But it seems like there are sort of a number of
18 things that folks would all agree on in terms of sort of
19 base level, physical security measures in terms of fencing,
20 and a number of other things that could be included as
21 regardless of whether it's in a rural area or downtown
22 Manhattan. We think we need at least this, and that they
23 likely show up in every single one of the mitigation plans
24 that's been developed under the CIP standards today.

25 And so I guess, and I also sort of stress this

1 because it's difficult from an optics and sort of public
2 responsiveness position, when incidents happen to say, you
3 know, what were the standards that they were following. And
4 while it's site specific, as it should be, but the following
5 question is always going to be there were no minimum
6 standards in place.

7 And the answer to today I think is no. And so,
8 I'd be interested to see if you think that we should be
9 moving towards at least some set of common sense, everybody
10 agrees exists in 90 plus percent of the mitigation plans
11 that are out there, set of minimum standards to be added to
12 the CIP framework.

13 PRESIDENT ROBB: It's a great point, and it's
14 certainly something that we're looking at as we kind of
15 complete this assessment. You know, one of the things we
16 want to look at is we had to go through the compliance
17 history around CIP 14 now. It is also fair to say CIP 14 is
18 a relatively fresh standard, so we don't have years and
19 years and years of history around it.

20 But I think the questions you raise are very good
21 ones. The other one I would put in place that we're talking
22 through is monitoring right? You know, should every
23 substation have a camera? Well and it turns out that that's
24 not as simple as you might think it is given EMF issues, and
25 so on and so forth.

1 So there's definitely work to be done. I think
2 there could be room here for a minimum threshold of
3 protection. We're not there yet, but that is certainly
4 something that could come out of this study. And I would
5 always come back and say there's nothing that would prevent
6 a state from imposing its own security requirements on any
7 of these assets.

8 So if to the extent that any of you feel that the
9 NERC standards don't go far enough to protect the systems
10 under your jurisdiction from issues that you're concerned
11 about, you can always go further. Right?

12 DR. RAAB: Commissioner Christie?

13 COMMISSIONER CHRISTIE: Yeah, for Mr. Robb I want
14 to follow-up on your statement that you can't harden every
15 substation in the country, the costs would be astronomical.
16 But I remember distinctly after the Metcalf incident in
17 California, which is what at least a decade ago.

18 I remember distinctly being briefed by Dominion
19 and there was a national effort ordered to prioritize those
20 substations that would have the greatest impact if they were
21 taken out, and of course the Metcalf station was at the top
22 of the list because it would have taken out Silicon Valley.
23 But not all of them rank up there.

24 What has gone on since then to do something like
25 that to do a continuous analysis of which substations are

1 the real high-value targets if you're, you know, on the
2 targeting end, and need to be defended more, whether it's
3 high-def cameras, whether it's armed guards, I mean there is
4 a hierarchy. I was told ten years ago that there's a
5 definite hierarchy, and if you focus on the ones that could
6 do the most damage if they go out, you can focus your
7 resources. Where does that stand?

8 PRESIDENT ROBB: So Commissioner, what you just
9 described is the essence of CIP 14, right? It was designed
10 to ferret out those assets that were -- that merited, you
11 know, a high degree of hardening. So I think the effort
12 that you're referring to was the effort to get CIP 14 in
13 place, and for the utilities to do all the work around that,
14 identify that short list.

15 COMMISSIONER CHRISTIE: Okay. And without going
16 into the law enforcement element, was the North Carolina
17 facility, where would that have ranked in CIP 14?

18 PRESIDENT ROBB: They were not CIP 14 compliant.
19 They were not CIP 14 qualified substations. And the fact
20 that that was -- and this is, I don't want to sound callous
21 here, because 40,000 people on a cold night in December
22 that's a huge customer impact.

23 COMMISSIONER CHRISTIE: Right.

24 PRESIDENT ROBB: The fact that that event didn't
25 cascade I think also reflects the fact that that risk

1 assessment was probably done properly.

2 COMMISSIONER CHRISTIE: Okay.

3 DR. RAAB: Any other questions or observations
4 the Task Force Members want to make on this before we keep
5 moving? Okay. So next we're going to do the next two
6 topics together, and we're going to let Director Kumar take
7 the lead. So the first is what are the best practices for
8 addressing physical attacks on the transmission system?

9 Be it restrictions on physical access, risk
10 assessments, surveillance? And categorically speaking, are
11 there prevention, detection, hardening, and recovery
12 practices that should be more broadly considered? And then
13 the next question, which we're going to do together, what do
14 recent attacks reveal about the effectiveness of existing
15 regulatory standards or best practices for physical
16 security?

17 And you were just responding to that a little bit
18 Mr. Robb, and are there opportunities to improve current
19 regulatory standards, or voluntary practices to minimize
20 risks and vulnerability, and respond to physical attacks and
21 restore service more quickly?

22 DIRECTOR KUMAR: Thanks for the question. So
23 just taking a step back real quickly because this ties into
24 what Jim was just saying, and the conversation we were just
25 having. You know when you think about what do you need to

1 do in terms of hardening of some of these substations. You
2 know there are two big approaches, right?

3 One is requirements, and that's CIP 14. It
4 certainly has requirements for monitoring critical
5 facilities, preventing attack or access, and otherwise just
6 hardening those facilities so that they are more physically
7 secure to protect against an attack or equipment failure.
8 That's bucket one.

9 Bucket two is taking the approach of making the
10 broader power system more resilient, which they have a
11 connection there. So on the first one we work with NERC on
12 a tool called the design basis threat tool. And the idea
13 behind the tool is utilities can leverage this tool on a
14 voluntary basis, and really evaluate the physical security
15 measures they need to take place -- they need to put in
16 place, for specific substations.

17 And it's really important to not just have a
18 blanket, everybody does the exact same thing because
19 substations as this community knows well, are in different
20 geographical regions. Some are near highways, some are
21 farther away from highways, some are at a higher elevation
22 or a lower elevation, and you have to take into account all
23 of those different aspects when you think about how you
24 want to harden that specific substation.

25 And so we provide this tool, and it's informed by

1 research, by the Pacific Northwest National Laboratory who
2 has expertise in this, and it's informed by intelligence
3 that we have to say here is the latest in the design basis
4 threat. That tool is updated on an annual basis. And I
5 would certainly encourage those utilities to take a look at
6 the tool, and it's available on the E-ISAC site portal.

7 Now in the second piece, how do you make the
8 system more resilient, so that if you do have an incident
9 like this you can ensure the resiliency of the grid more
10 broadly? There was a Congressional Research Service report
11 from 2015 titled Physical Security of the U.S. Power Grid,
12 which has a quote from Mike Kormos of PJM, which I'd like to
13 share.

14 The quote is, "You can only harden a substation
15 so much. If someone wants to attack a substation, they
16 will. This leads us to the resilience piece. Maybe the
17 best way to make a substation less critical is to build more
18 transmission. A substation is critical basically because
19 we're pushing too much power through it."

20 So going back to my earlier comments of as we
21 think of the grid of the future, we can build in security
22 and resilience by thinking about the new distributed
23 generation, additional transmission, so that it doesn't
24 cause that large impact to customers. So in the case in
25 Moore County could we have looked at microgrid solutions,

1 and battery source solutions to be able to keep customers
2 online.

3 So again, I think we really do need to think
4 about both pieces of the actual specific physical measures,
5 definitely need to be thinking about them, but then also
6 really thinking about the broader resilience of the grid,
7 and to communities themselves.

8 DR. RAAB: Do you have any yes? Commissioner
9 Allen?

10 COMMISSIONER ALLEN: Thanks. I wasn't sure
11 exactly where to kind of fit my question in, but it really
12 concerns what I'll call the analytic basis that you go
13 through in kind of choosing different technologies to either
14 protect the system from a physical security threat, or to
15 address perhaps even all hazards type concern.

16 But my issue is really kind of looking at the --
17 and getting essentially the biggest ratepayer buck for the
18 investments. And from my standpoint it seems like it would
19 be helpful as we think about how we analyze ways to protect
20 the physical system, that we do it on a consistent analytic
21 basis.

22 And by that I mean kind of looking at and
23 comparing the alternatives, whether we're talking about the
24 protective measures, the hardening measures, or we're
25 looking at the things that you just alluded to, which are

1 more the back end mitigation, and rebound or resilience
2 qualities of the system.

3 But we do it on a basis that is, you know,
4 consistent. These impacts potentially cross state borders,
5 and potentially cross regional borders, and establishing,
6 you know, cost effective ways to do things seems sensible.
7 When I reflect back on the comments of Mr. Robb he referred
8 to CIP 14. He said this is a prescriptive process, but not
9 prescriptive on the mitigation measures.

10 And that seems like a very sensible approach.
11 But there's something in between, at least from my
12 standpoint, which is considering how we analyze these
13 things, and whether we kind of adequately incorporate, you
14 know, the things that extend beyond the physical system, as
15 we look at the investment.

16 So to include things like consumer impacts, maybe
17 even community impacts, which can exact, you know, quite a
18 considerable impact broadly. I've had a chance to kind of
19 survey lots of my contacts in the industry, and there are
20 two points that they've kind of made that stand out to me,
21 and I kind of wanted your reaction to them.

22 I'm really focusing on Mr. Kumar right now
23 because I understand that this is the cost-effective issue
24 isn't necessarily squarely in the NERC frame, but it is just
25 a question of looking at, and establishing a sound

1 definition for resilience, measuring resilience, perhaps
2 quantifying, and monetizing the resilience measure, and
3 whether we can do better in terms of looking at consumer and
4 community impacts.

5 DIRECTOR KUMAR: Commissioner, thank you for the
6 question. So for a very long time we've done a good job of
7 being able to quantify climate based risks. We have
8 historical data on that. We have really good information to
9 say if you apply this measure you can buy down so much of
10 the climate risk.

11 If you harden this infrastructure you could do
12 that. With the growing physical threats, and I would add
13 cyberthreats that we're seeing, we don't have great models
14 along those lines. That is an area we need to be thinking
15 about, not only from, you know, a broad level, at the
16 Department of Energy, and that is something we are focused
17 on, is how do we really better leverage data and analytics
18 to help quantify some of these risks, so that then you can
19 compare them against the investments you need to make and
20 decide whether you want to add more dollars here, or more
21 dollars there, particularly on the physical and cyber risks.

22

23 And so that's an area we're really focused on,
24 and would like to do more work on, and hopefully the goal is
25 to provide the information not only to the owners and

1 operators, because they're making their own risk decisions,
2 their own investment decisions, to be able to arm them with
3 the information that we have to do that, but also our
4 colleagues in the regulatory community.

5 It's you all at the state level, at the federal
6 level, so that standards could be adjusted based on that
7 understanding of risk. Now one piece of the puzzle that we
8 need in all of that is reporting. We need to intercede. We
9 need reporting of when these incidents happen. Certainly
10 we're getting some of that reporting, but that's a really
11 key piece that we need to ensure that utilities are
12 reporting these incidents, even if they seem like minor
13 blips.

14 If it's just basic vandalism we still need to get
15 that reporting so we can see the larger trends, and get the
16 data, and then based on that data be able to help develop
17 some quantifiable measures, but I think that's an area where
18 we need to continue doing more, so thank you for the
19 question. It's a great one.

20 DR. RAAB: Other questions or observations,
21 comments from Task Force members? I was going to turn to
22 you and let you. Yeah, go ahead.

23 PRESIDENT ROBB: Yeah, I know, I'm sorry. I just
24 wanted to foot stomp something that Puesh said that's really
25 important, and to the extent that you could encourage those

1 utilities on the jurisdictions, the more reporting we have
2 into the ISAC the better. And I recognize that sometimes
3 there may be some concerns about reporting things into the
4 government, and so on and so forth.

5 But report to the ISAC. One of the things that
6 we've seen happen, particularly around some of these
7 clustered events in the Northwest is that our physical
8 security team has the ability to take and triangulate
9 events, and see patterns that others don't. And it's one of
10 these questions where no event is too small, because what
11 may appear inconsequential to one utility, could be part of
12 a broader pattern.

13 And we've actually seen some things that we
14 worked with the National Counterterrorism Center at
15 uncovering some things that were very curious, and led to
16 some kind of very proactive things on behalf of law
17 enforcement. So the more data we have, the more insights we
18 have, the more information that gets shared, and the ISAC
19 creates a safe, you know, user controlled way of sharing
20 that information the better.

21 So I would encourage you all to encourage your
22 entities to report as much as they can.

23 DR. RAAB: Commissioner Allen?

24 COMMISSIONER ALLEN: Thanks. It's just a
25 follow-up actually to Mr. Kumar's comments. You know, I

1 took to heart his comments that, you know, we have to build
2 -- there are building blocks that need to be put in place to
3 establish a, you know, a credible and defensible, analytic
4 frame, and a consistent framework.

5 I think there are kind of efforts. I think the
6 National Labs are actually doing some pretty good work in
7 this space, and I think that can be combined with, you know,
8 techniques that are being used by some of the utilities on
9 the probabilistic, and to kind of meet the challenge. But
10 assuming we can of get through those challenging building
11 blocks, does it make sense to put in place, you know,
12 establish you know, a consistent, analytic framework?

13 And if it does make sense, where would that come
14 from? Would that come from NERC, FERC, DOE, how would you
15 establish that for the bulk transmission system if you can?

16 DIRECTOR KUMAR: So if we were to work on
17 something like this, it would have to be done
18 collaboratively. You know, certainly we have the tremendous
19 capabilities at the National Laboratories as you mentioned
20 sir, but we also need the expertise of the owners and
21 operators that know their substations, know their systems,
22 and so we need to come together as a community.

23 Jim mentioned the Electricity Subsector
24 Coordinating Counsel, or the ESCC. That is a body that
25 brings together industry and government together to tackle

1 these hard problems of security and resilience. That is
2 what they are squarely focused on, and so that could be a
3 venue or a space to bring us together to really think about
4 how we look at some of these investments, and what more we
5 could be doing, so that would be an idea I have.

6 DR. RAAB: This rolls into the last question,
7 which is what are the respective roles and responsibilities
8 among the federal agencies, and between federal, state, and
9 local governments when it comes to the physical security of
10 the transmission system.

11 And how in your opinion can the states, FERC and
12 other government agencies and utilities work together to
13 identify transmission system assets that require greater
14 protection, and ways to address that need for greater
15 protection? You mentioned sharing information, can you
16 build on that? You first, and then.

17 DIRECTOR KUMAR: So broadly DOE, and specifically
18 my office, the Office of Cybersecurity, Energy Security and
19 Emergency Response, is designated as the sector risk
20 management agency, or the SRMA, for the U.S. energy sector.
21 In that role our focus is to work and partner with not only
22 owners and operators of electricity, oil and natural gas
23 infrastructure, but also the state and local, territorial
24 and tribal community.

25 And so we have tremendous partnerships with our

1 colleagues at NARUC with the energy offices, Governors
2 offices, and we recognize that we have to be working with
3 everyone to think through all these security and resilience
4 risks, and then also collaboratively work with them to buy
5 down those risks. Again, either through the policy side --
6 earlier today we partnered with NARUC to announce an effort
7 to develop cyber baselines for the distribution system.

8 And this is an important partnership as we think
9 about it. So in our role we're kind of the convenor across
10 the energy sector, and we work with our colleagues at the
11 Department of Homeland Security, with the Federal Bureau of
12 Investigation, and other agencies to ensure we have a whole
13 of government coordinated approach, but really we focus on
14 specifically energy.

15 And in that case we're working with our
16 colleagues at NERC and FERC in terms of the regulatory
17 requirements with the PUCs and PSCs on this state regulatory
18 piece, but also with the energy offices on their resilience
19 conversations that we were talking about earlier. So we
20 really do have to work with everybody on securing this
21 infrastructure going forward, and this is critically
22 important, and particularly as we think of the transmission
23 system.

24 Certainly the transmission system of today, and
25 how we need to expand the transmission system of tomorrow to

1 be able to connect all these assets to going back to the
2 reliability and redundancy and resilience conversations
3 we've had.

4 PRESIDENT ROBB: Yeah. I think I agree with
5 everything Puesh just laid out. The one thing I'd maybe
6 expand a little bit, I think it's important that we bring
7 law enforcement to the table, whether that's at the national
8 level, regional, or local level. State police departments,
9 local police departments, FBI, because I think like in many
10 of these hazards prevention is worth a pound of cure right?

11 And if we can kind of figure out, you know, where
12 plots are being formed, particularly and it's really the
13 coordinated attack is what really spooks me about our
14 current set of standards versus where we might need to go.
15 And the more we can get and gain confidence that things like
16 happened with Baltimore plot revealed earlier this week
17 where we can have confidence that law enforcement can
18 understand and disrupt before an event takes places, so much
19 the better.

20 Because trying to again, harden the
21 infrastructure against that is going to be very expensive.
22 I think that's really important. The second thing that I'd
23 say is I do think Commissioner Allen you're on to something,
24 and I think the more a standardized or agreed approach for
25 doing the risk assessments, which is broadly shared.

1 And I don't know that that's appropriate to be
2 baked into a NERC reliability standard, because that brings
3 a lot of hair with it. But I think conceptually that makes
4 tons of sense. Because one of the things I'd like to be
5 able to see here that is similar to what we have with our
6 emergency operations restoration planning, is that you
7 create a framework for the utilities to be able to have a
8 structured conversation with their local utility commission
9 around, you know, what our response is if we found ourselves
10 in one of these situations.

11 And then you can have a pretty intelligent
12 conversation around are we willing to wear that risk, or are
13 there investments we should make that would mitigate that?
14 And ultimately again, I think that conversation is always
15 going to be best held at the state level, but it's got to be
16 informed by something.

17 And I think the more there were a standardized
18 approach for doing the risk assessment, probably the greater
19 confidence, you would have in the greater confidence the
20 utility would have at their ability to kind of work through
21 therefore, here's what makes sense in our context, which
22 again would be very, very, different, you know, if you're
23 thinking about an urban area versus a rural area, you know,
24 and so forth.

25 So I think that's something we'll take onboard.

1 DR. RAAB: We just have a few more minutes, and
2 I'm just wondering in some ways the biggest ball in this
3 area is in your court right now at NERC, with a report due
4 at FERC in April. And I'm just wondering if you have any
5 question that you wanted to ask the Task Force, or to get
6 some feedback on that would be helpful for you as you're
7 moving forward?

8 PRESIDENT ROBB: I wish I had known you were
9 going to give me that opportunity Jonathan, and I would have
10 prepared a little bit more thoughtfully. Look I think I
11 would love to hear what the states would find helpful in
12 this area. Again, I think our statutory authority given to
13 us by Section 215 of the Federal Power Act in this area are
14 fairly clear.

15 I suspect they are completely insufficient
16 relative to the issues that are of concern to a State
17 Commissioner, right? Because we're really trying to protect
18 against the 40 million customer outage, right, and you all
19 have to worry about 40,000 customer outage. I get that.

20 And so I guess the questions that I would open
21 the door either now, or in subsequent conversation, you
22 know, feedback is what the states would find helpful, right,
23 that doesn't provoke any sort of a jurisdictional war,
24 because I don't think any of us want to do that. But things
25 that we can do that would help advance the ball in your

1 courts I think would be very, very helpful for us to
2 understand.

3 DR. RAAB: So Chair Stanek had his card up before
4 I asked that question, but why don't you go ahead and then
5 Chair Dutrieuille, and then Chair Scripps.

6 CHAIR STANEK: Yeah. Appreciate that. There we
7 go. I appreciate those comments Mr. Robb and Mr. Kumar, the
8 whole of government approach. Obviously, this Task Force
9 we've greatly improved relations with FERC over the past two
10 years. We had the offer of assistance from Joe McClelland,
11 Director of OEIS at FERC who provided us with a wonderful
12 presentation on Sunday.

13 Obviously, the Baltimore incident is fresh in my
14 mind, and I'd like to just thank the U.S. Attorney's Office,
15 Department of Justice, FBI, for all of the hard work that
16 they've done. In terms of both NERC and DOE, where do you
17 view the State Commissioners as fitting in? And whose
18 responsibility at the federal level is it to outreach to
19 State Commissions when an incident such as Moore County, or
20 Baltimore occurs?

21 DIRECTOR KUMAR: I can take that one. So where
22 Jim started some of these incidents become very sensitive
23 very quickly depending on the nature of the incident right?
24 There's a criminal investigation that ultimately ends up
25 happening, and so as my law enforcement colleagues remind me

1 often, that this is -- it's handled delicately because even
2 in the case of the incident in Baltimore Gas and Electric
3 and Exelon service territory, or the plot that is, they are
4 going to court now, and right now there is an indictment.

5 There is going to be a full proceeding, and so
6 they want to protect that investigation. And so it does
7 become delicate in terms of when information is shared.
8 With that said, we do have to ensure that we have
9 established protocols for sharing information, and I think
10 that goes not just for physical, that should also go for
11 cyber.

12 How do we make sure that the right offices in the
13 states have the information in the appropriate timeframes?
14 And so I know Jon you didn't ask me for a question for the
15 Commissioners, but that is a question I would ask the states
16 as well. When would you like to be notified? What are
17 those requirements?

18 Now do you want every single incident? Or is
19 that noise? Or does it hit a certain threshold when it
20 would be beneficial for you all to know. That is a
21 conversation I've had with other states, but I'd love to say have
22 a process that we could potentially look at having across
23 the country. It might not always work in every state.
24 Every state is different. I recognize that.

25 But if we could be thinking about an approach as

1 to what are those thresholds where you would like to be
2 notified. Now there is another challenge to all of this.
3 It also depends on who you are talking to in the state. In
4 some cases it's the homeland security advisors that might
5 get told first, as opposed to the utility commissioners, or
6 the energy offices.

7 And so that dynamic also exists, and so I've said
8 this earlier today, and I've said it over the weekend at the
9 National Governor's Association. I think that's an area at
10 the state level where we would love to partner with you and
11 bring together both Governor's offices, homeland security
12 advisors to really be thinking about that well before cyber
13 and physical incidents, in terms of who gets the reporting,
14 and how does that get out to the utility commissioners.

15 And I would add the energy office as well, but
16 it's a good question, and we still need to do more work on
17 that.

18 PRESIDENT ROBB: Can I make one observation?
19 This may not be directly responsive to your question
20 Commissioner Stanek, but I think it's important. We, every
21 two years, run this massive security exercise we call Grid X
22 right, where we break the grid, and we work with our
23 government partners to figure out how would we actually work
24 through restoration, and who has what authorities to do what
25 then, and so on and so forth.

1 It's always a highly instructive exercise. To
2 the extent that you're not doing those, I would encourage
3 those to play out at the state level right, because you will
4 learn through that, you know, where your soft underbelly is,
5 what processes need to be shorn up, what relationships need
6 to be built, you know, both among the private sector, among
7 the public sector, in between.

8 And those would be very, very useful exercises to
9 do. The other thing that, again, I will continue to harp
10 on, the more folks can share information with the ISAC, even
11 if it's not particularly clear or actionable, because we can
12 share that more broadly as well, and do it in a way that's
13 confidential, and protect identities and all that kind of
14 stuff.

15 So the ISAC can be a very, very important tool
16 here for both doing reconnaissance, as well as you know,
17 putting people on alert that need to be put on alert.

18 DR. RAAB: Chair Dutrieuille and Chair Scripps
19 your wish list.

20 CHAIR DUTRIEUILLE: They've been talking about my
21 wish list. It's been interesting. I'm going to start with
22 answering the question that Mr. Robb had asked in terms of
23 what do State Commissions want. And then Jason asked his
24 question and gave his comment, and it was going back and
25 forth. So what I was going to say, and you've answered some

1 of it, even with some of the questions that you presented,
2 is communication is key to us. But it's different in every
3 state.

4 And so as you were mentioning in terms of some
5 states have different state energy offices than what the
6 PUCs are, which is the case in Pennsylvania. Sometimes the
7 information is presented through to the emergency management
8 agency first, and then the Energy Office, and then the PUC
9 may come third, fourth or fifth down the road.

10 So it is very important that we also receive the
11 information, and trying to figure out how to coordinate it
12 properly. Once again I say every state is different, so
13 it's still important because eventually it's going to get to
14 the PUC, and they're going to ask why didn't we know. So
15 that is my wish list.

16 DR. RAAB: Chair Scripps?

17 CHAIR SCRIPPS: So I think there's two things.
18 One, on the reporting piece I think there's room both for
19 information sharing between the federal and state, and I
20 think you're right to say that there's probably different
21 pieces of both of those. I also think there's probably more
22 we can do in terms of reporting on physical incidents.

23 We have updated in Michigan our cyber rules
24 recently that require annual check-ins with the utilities
25 just to get a sense of sort of the threats they faced over

1 the previous year and then more immediate reporting where
2 there is loss of service, extortion, data breach, et cetera.
3 I think there are probably analogs to that, and in the
4 physical space certainly loss of service, but and then
5 there's something of a judgment call where whether even if
6 it falls outside of the defined categories, if it's a
7 serious incident, and there's some judgment in there, that
8 that gets reported immediately as well.

9 So I think there's ways that we can work to
10 implement similar protections on physical security. But Mr.
11 Robb when you were talking about some of that it sort of
12 called to mind some of the shared responsibility around gas
13 safety, and gas safety is obviously very different. But
14 you've got an explosive element in the pipes, and we need to
15 make sure.

16 But the way that we implement this at the state
17 level is under delegated authority from DOT PHMSA where we
18 have gas safety specialists who are regularly out in the
19 field checking on the infrastructure. And it seems to me
20 that there may be some role for similarly delegated
21 authority to the states to do sort of an evaluation of CIP
22 compliance.

23 This is not to say that there's any bad faith in
24 the industry. I think that CIP is working because of the
25 good faith application, but it's always good to have -- get

1 another set of eyes, and particularly from the regulators
2 that as Chair Brown Dutrieuille mentioned, are going to be
3 called when incidents do happen.

4 And so, developing some sort of similar framework
5 with delegated authority, and I would say funding, to allow
6 and enable State Commissions to perform a similar role on
7 sort of just investigating CIP compliance as we do on
8 compliance with gas safety standards may be a direction that
9 we might want to consider.

10 DR. RAAB: Commissioner Christie, or did you want
11 to make another comment, or is your card up from before?
12 Okay. So we're a little bit over time, so I think we're
13 going to say thank you very much to both of you, and we'll
14 take a ten minute break, and we'll start at 2:55. So hurry
15 up and do whatever you need to do because I know coffee is
16 far away, right?

17 (Break.)

18 DR. RAAB: So, now is our opportunity to hear
19 from us and have a discussion among the Task Force members
20 on these issues and we'll be, I'm sure, touching on some of
21 the things that we've heard from them and that some of the
22 Task Force members points they made and had a chance really,
23 kind of, kick the tires on some of the ideas that were
24 coming up and we've divided it into two parts, the first one
25 is on planning and planning to address threats and

1 vulnerabilities to the physical security of the transmission
2 system. We have two questions on that, and then we'll move
3 to enhancing coordination which we're also touching on and
4 other potential changes.

5 So, starting with planning, as everybody knows,
6 we've had two Task Force meetings already focused on
7 planning, one on intra-regional and one on inter-regional
8 planning and there's an NOPR out that largely deals with
9 planning, so now we're kind of thinking about layering in
10 the physical security issues to the really robust
11 discussions that you've already had on planning. And the
12 first question that we want to explore, is, are there
13 opportunities through the regional and local transmission
14 planning and state review processes to address threats and
15 vulnerabilities to the physical security of the transmission
16 system?

17 For example, by addressing aspects of the
18 transmission system topology that makes certain transmission
19 assets particularly vulnerable or other things. And so,
20 we're going to start with Chairman Phillips is going to
21 start, then Commissioner French and then Commissioner
22 Gillett from Connecticut.

23 CHAIRMAN PHILLIPS: Thank you, Dr. Rabb, I really
24 want to hear from my state colleagues, so, I'll be very
25 brief on this one. You know hearing the discussion and

1 responding to what we heard earlier to, you know, to think
2 about Jim Robb saying they're worried about 5% of the
3 attacks they see. I think we have an opportunity, but I
4 think we need to be balanced. We need to balance it with
5 cost and affordability, but I'm reminded of something, I've
6 recently reconnected with my trainer, thinking about
7 something that's critical, right? And they told me
8 something, they said this, you can either pay me now, or you
9 can pay the doctor later. And I think about how we view
10 physical security now. You know, it's sort of like an after
11 the fact bolted on type of process that we're doing. But if
12 we bake it in now. If we consider it on the front end, I
13 think we do have an opportunity to do something about what
14 could be a very costly process if we have some of these
15 coordinated attacks that you heard our presenters talk about
16 earlier.

17 You know, one thing that DOE talked about that I
18 think was very, very thoughtful, is reducing the criticality
19 of particular facilities. I think PJM, they have a CIP 14
20 project mitigation process that they're going about right
21 now implementing, and I think that there are lots of
22 arguments around identifying what these facilities are, and
23 we can talk about keeping that information confidential.

24 And if you sort of, you know, plan for that
25 component of the reduction of criticality, I think there's a

1 lot to be gained in that process, and of course, David
2 Ortiz and Joe McClelland at FERC, they can talk to you all
3 day about the specifics of what to do, but those are the
4 general thoughts and ideas that I have.

5 DR. RAAB: Commissioner French?

6 COMMISSIONER FRENCH: Thank you. I think you're
7 going to hear a similar theme in my remarks. And I'm not
8 going to say anything brilliant here. I'm glad we were able
9 to hear from some of the experts to begin with. I think
10 that was the most important part of what we were able to do
11 today, and probe their thoughts.

12 I certainly share, you know, a lot of the
13 sentiment that the answer to a lot of what we're talking
14 about, it's not tacking on, you know, new technology onto
15 every single substation. It's about eliminating targets,
16 and I'll repeat what I said earlier. I think we have a
17 system that's already very resilient by its very nature.

18 The fact that it's so decentralized and meshed,
19 and looped, we don't have a lot of targets, but there is
20 always room to improve, and to evaluate where we could
21 become more decentralized, and figure out where those spots
22 lie. The specific question here lies with the regional
23 planning process, and local planning processes.

24 And I think, you know, if we were talking about
25 investments to further decentralize the grid, I do think,

1 you know, the RTOs, or the regional planning processes are
2 an appropriate place to do that planning. Those, at least
3 in my neck of the woods, those are vigorous transparent
4 stakeholder processes, that really suss out the lowest cost
5 option, you know, as far as a new facility, particularly if
6 it's going to be a regional facility that may have
7 significant costs associated with it.

8 I think there's a big benefit to running that
9 through the stakeholder process. Obviously, with the
10 appropriate confidentiality protections that might flow from
11 something that attaches to physical security. But yeah, I
12 think that can be worked through. We also have local
13 planning criteria that will look at things like, you know,
14 radial versus looped lines, and the resiliency that goes
15 into that.

16 And I think that's an appropriate place to look
17 at that. So I do look at this from the cost perspective of,
18 you know, if there are upgrades necessary, and nobody is
19 presupposing that any level of upgrade is necessary, but if
20 there are, I think those transparent processes that subject
21 investments to quite a bit of stakeholder scrutiny, we
22 should try to use them as much as appropriate for a
23 sensitive issue like this.

24 DR. RAAB: Commissioner Gillett?

25 COMMISSIONER GILLETT: Thank you so much. I

1 appreciate the opportunity to provide some remarks about
2 this topic. I want to start by saying I think a little bit
3 of what I heard from Chair Phillips in terms of responding
4 to rate payer concerns. And when I was considering this
5 topic, you know, I think what we're hearing from ratepayers
6 in Connecticut, and probably throughout the Northeast given
7 the high prices, particularly those that went to effect
8 January 1 of this year.

9 You know the ratepayers do not care whether their
10 power is out because a squirrel chewed through the line, or
11 because a plant went offline unexpectedly, or you know, in
12 this instance that the substation might have been
13 sabotaged, or some other kind of difficult security event.

14 So the reason I highlight this as my first
15 comment on this subject is when it comes to things with the
16 transmission system and other things that are not
17 necessarily within state regulators' direct control. I
18 personally feel frustration at times because our ratepayers
19 are holding us accountable for these assets and their
20 failures.

21 When I think we struggle sometimes to think about
22 how or where we fit in to this planning processes. And I
23 told Commissioner French that I think some of the regional
24 planning processes, and RTO processes that do exist today.
25 Certainly, not looking to replace those, or duplicate

1 those, I don't want to waste any resources, but I do want to
2 offer, you know, at least speaking from, I'll speak from
3 Connecticut's perspective for one moment to say that I think
4 we've had some challenges and issues with respect to the
5 governance structure, you know, of our regional
6 transmission organization.

7 And specifically, sometimes frustrations that the
8 state doesn't always feel like it has a seat at the table
9 when it comes to some of those planning processes. So I
10 worry about utilizing those planning processes to insert
11 considerations about physical security particularly if
12 they're bolted on, you know, after the fact, which I don't
13 think anyone is suggesting they are here.

14 But if we have to maintain the confidentiality in
15 those types of discussions, I worry that bringing that into
16 the planning process is going to provide a kind of a
17 convenient excuse at times to take some of those conversations
18 off line, or if, you know, especially out of the earshot of
19 certain parties. And I just think we should be cognizant in
20 putting guardrails and objectives around what those planning
21 processes are still there to achieve, which in you know, my
22 opinion is get to the least cost, or most cost-effective
23 outcomes that we can.

24 So you know, I want emphasize still that I
25 recommend that the planning processes, you know, are

1 probably the right place for these discussions to be
2 applied. I just think we need to be cognizant of some of
3 the challenges around them, especially because of that
4 tension between the openness, between wanting to have
5 openness planning, while needing to discuss the concerns
6 about disclosing too much about physical security threats in
7 public.

8 So you know, in sum I think definitely
9 opportunities to address this regionally. Just want us to
10 be careful as we're setting that up, which is I know, why
11 we're all here today to discuss. So I'm going to stop
12 there, and thank you so much.

13 DR. RAAB: Thank you all for the open comments.
14 Others want to jump in on this, are there things that can be
15 layered into the planning processes we've been talking about
16 to reduce the criticality of facilities and the long-term
17 planning benefit streams, all the things that we've kind of
18 touched on, and are in the NOPR. Yeah Chair Stanek?

19 CHAIR STANEK: Thank you Dr. Raab. Just a quick
20 anecdote that actually Joe McClelland mentioned on Sunday.
21 The 80/20 Rule, the Pareto Principle. The fact that if in
22 the planning stage we spend 20 percent more, whether it be
23 gates, guards, guns, Kevlar, ballistic walls.

24 We could receive or avail an 80 percent return on
25 that 20 percent investment. So I think planning, especially

1 new infrastructure, we can bake that in, obviously it's more
2 expensive to do a retrofit for existing substations, but
3 it's something obviously to consider, certainly the cost
4 benefit of putting up whether it be fencing for lower value
5 targets, or something more expensive for higher value.

6 DR. RAAB: Others? Commissioner Allen?

7 COMMISSIONER ALLEN: Yeah. I'll just feed off of
8 the little bit of what Mr. Kumar said, and Chair Gillett
9 mentioned, which was you know, just building things, in I
10 think upfront in the planning processes, whether they're
11 local planning processes, or regional planning processes,
12 are fairly beneficial and I will have some remarks on kind
13 of how to do that. But I really like the path of thinking
14 long-term, incorporating as Chair Stanek had mentioned.

15 The extra steps early, and minimizing dependence
16 of bolting on afterwards approach that has already been
17 discussed.

18 DR. RAAB: Okay. Seeing no others, we will move
19 on to the next question, which is how should the state and
20 federal regulators assess the benefits or the value of
21 potential investments that can be weighed against costs?
22 And maybe less certain benefits and values with maybe
23 clearer costs to address threats and vulnerabilities to the
24 physical security of the transmission system.

25 And again, we've talked a lot about what benefits

1 should be looked at, and how to really assess things. This
2 is maybe a slightly different animal; how should it be, how
3 should it be done in particular, how do we identify the
4 values of avoiding. And so we do have some people. First,
5 Chair Pridemore and then Commissioner Allen, and then
6 Commissioner Clements.

7 CHAIR PRIDEMORE: Thank you Dr. Raab. So state
8 regulators should assess the value and benefits investments
9 to address potential vulnerabilities to physical security in
10 our respective states. State regulators should encourage
11 utilities to build upon existing NERC standards such as CIP
12 14, to address internal vulnerabilities, increase background
13 checks, including digital and financial.

14 To address external vulnerabilities, table top
15 drills with state partners, such as your emergency
16 management partners, Department of Transportation, and
17 others, and participate in the nationwide NERC exercise
18 drills.

19 Vertically integrated non-RTO states, such as
20 Georgia, have robust integrated resource planning, and we
21 have the ability to remove any barriers to coordination with
22 state and federal partners. Another benefit is that the
23 analysis and evaluation of transmission costs, we can do
24 that alongside generation costs in our rate cases.

25 We can do so without having to be concerned with

1 top of stack pricing. In Georgia, the dollars spent on
2 transmission also allows more renewables to be built at a
3 lower cost. Beyond existing efforts, State Commissions
4 should work with their legislatures to evaluate and
5 potentially increase penalties for criminal interference
6 with critical infrastructure.

7 All five Georgia Public Service Commissioners
8 support Georgia House Bill 227, which was dropped just in
9 January. It will increase the penalties on these criminal
10 actions, and move them to felonies. We believe that this
11 increase in penalties acts as a deterrent, and we also
12 believe that it will prove that Georgia takes physical
13 security of critical infrastructure seriously during these
14 times.

15 Lastly, may we all do our best to guard that
16 which has been entrusted to our care. This is important to
17 our states. This is important to the people that we
18 represent, and we can do so without gold plating.

19 DR. RAAB: Commissioner Allen?

20 COMMISSIONER ALLEN: Yeah. So I think I've
21 already telegraphed what I have to say, but I'll try to
22 expand on it a little bit. I mentioned three points
23 essentially. One is I think we need to really, you know,
24 clarify and in a sense, nail the concept of resilience. In
25 my mind there's some really good academic work that is out

1 there, that covers the various dimensions of resilience.

2 The one that works for me is one that recognizes
3 kind of the hardening as an element, the mitigation and
4 limiting duration, and the rebounding from events when they
5 occur. The latter two in my mind are best kind of viewed in
6 the broader frame of not just physical security threats, but
7 in, you know, a more robust framework that considers,
8 especially weather and other hazards that are out there.

9 And that in my mind fits very well into, you
10 know, the kind of analysis that we do long-term on an every
11 two or three year basis, but looking out, you know, ideally
12 over the very long-term. So I would prefer a minimum of 20
13 years, but that's the subject of another NOPR, and I won't
14 go too far down that, but just to say let's address it as
15 much as we can on the front end.

16 So a clear, robust, consistent framework. I
17 think that means metrics, it means quantifying, I think it
18 actually means monetizing the values as well. And I think
19 the building blocks that we had talked about earlier are
20 actually getting pretty well formed. The National Labs are
21 doing really good work. They need some, you know,
22 additional monies, and in order for it to really to improve
23 what they have.

24 But the industry, to varying extents, have been
25 relying on some of these building blocks over time. They

1 just need to be made better and more robust, more
2 compelling, and I think it's fundamentally needed because I
3 think state regulators really require that kind of, you
4 know, solid and firm quantification when we're, you know,
5 anguishing over how we use rate payer dollars.

6 The second point is I think greater consideration
7 should be given to making the cost effectiveness analyses
8 more robust. I like a formal cost benefit analysis that's
9 consistent with my comments around resilience when we were
10 making investments in resilience activities.

11 We need to do our best to actually to try to
12 recognize the first order impacts on the system, the second
13 order impacts on the consumer side of outage, and then
14 subsequent order impacts on the community at large, which
15 can be a value added, and can be on physical health and
16 well-being of the community.

17 The third point -- well the third point I will
18 make is really just what I just said, which is a robust
19 analysis in my mind, does recognize the consumer side of
20 these impacts. And what we have presently are tools that
21 are, you know, are available, that do a pretty good job of
22 capturing the very short-term impacts, and willingness to
23 pay to avoid problems. I think they're now outdated. They
24 need to be improved.

25 We need to invest in the benefits that need to be

1 calculated, either on behalf of consumers, be that loss in
2 production from a commercial or a manufacturing facility or
3 the inconvenience in the short-term, but potentially much
4 more severe impacts as we move toward electrifying our
5 buildings, and transportation system.

6 The costs are going to go up of outages, and we
7 need to do good work to get ahead of that as much as we can,
8 and incorporate in the planning frame. Thank you.

9 DR. RAAB: Commissioner Clements?

10 COMMISSIONER CLEMENTS: Thank you. Listening to
11 Mr. Robb and to Director Kumar, I'm decidedly encouraged
12 each time I hear them speak. I do think that the federal
13 government is not just talking. They're really making
14 improvements in the coordination across these agencies,
15 including the law enforcement intelligence agencies, in a
16 really important fashion, so I like that starting point.

17 That's optimistic. When I think about this
18 question I think it's our job to keep asking questions, and
19 then try and put some parameters over how long we're going
20 to ask the questions before we decide whether or not
21 there's action to take, and all of the State Commissioners
22 who have just provided comments are putting really good
23 points into the conversation.

24 So I just have two short points. One is let's
25 get this data. Let's keep getting the data. Let's do what

1 Mr. Robb asks, and let's report these incidents. For me,
2 how do we then take that data and land on the right level of
3 risk? Because if each state has a different perspective,
4 and knows the things that their state needs, and at the same
5 time we're looking for a way to improve efficiencies, and
6 increase efficiency across the states relative to the FERC
7 jurisdictional piece of this puzzle, how do we land on the
8 right level of risk in that stage?

9 And that's something that I think, hopefully, the
10 NERC report will inform, and help us with. And then, you
11 know, there's this question of how much consistency we want.
12 I think we shouldn't rely for the bulk electric system on
13 just saying if the states aren't happy, they can just add
14 more. That leads to 48 different standards relative to that
15 piece.

16 The second piece I think is something Director
17 Kumar said, and you've just emphasized Commissioner Allen,
18 the overlap between at least the restoration piece, and to
19 some extent the mitigation piece of resilience that crosses
20 over the types of risk we're talking about. The climate
21 risk, in addition to the physical risk and the cyber risk.

22 And so for backing up to the planning timeframe,
23 that feels a little daunting to try and figure out how to
24 incorporate that into the planning timeframe, while keeping
25 that customer protection in mind because how far do you open

1 up? This is a new kind, another kind of value to
2 multi-value planning, so how do we open that up?

3 But I would just second the notion for your
4 robust cost benefit analysis and to try, even if it's kind
5 of running shadow analyses up front to understand what it
6 would look like in any decision that we're making or
7 deciding not to make, and using that data to help guide us
8 forward. I think that would be, perhaps, a starting
9 approach, so thanks.

10 DR. RAAB: So others who want to add, second,
11 disagree with anything that you've heard on this issue about
12 valuing? We'll move on. Okay. We're going to move on to
13 the last piece of our presentations, and hopefully some more
14 discussion on enhancing coordination of the potential
15 changes. We've heard a lot of references to better
16 coordination, better information sharing before.

17 So the question is how can the states, FERC, and
18 other government agencies and the utilities work together to
19 identify transmission system assets that require greater
20 protection, and ways to address that need for greater
21 protection.

22 For example, is there a need to improve
23 information sharing among these entities, recognizing
24 necessary restrictions on the share of confidential
25 information, which numerous people have said how do we do

1 this? What needs to be done, and how do we do it in a way
2 that will work?

3 So we have starting off with Chair LeVar. And
4 then Chair Dutrieuille, and then Commissioner Houck, and
5 then Commissioner Christie. I have a lot of volunteers for
6 this one.

7 CHAIR LEVAR: I'm going to just take a moment or
8 two and make what I'll call a soft suggestion, and it's
9 directed towards FERC and NERC to consider encouraging the
10 NERC regional entities to explore compliance data that can
11 appropriately be shared with state regulators, and also to
12 explore whether there's data in the hands of state
13 regulators that would be useful to these regional entities.

14 In the west, the regional entity WECC is going to
15 great lengths to become a stronger resource to state
16 regulators. They are sharing significant data with
17 stakeholders across the west on issues like resource
18 adequacy, historical trends on demand capacity, and
19 resources, and generation and transmission outages.

20 It's a bigger challenge to share aggregated data
21 on compliance, you know, high level impressions from audits,
22 spot checks, and investigations that the regional entity
23 does, and finding ways to aggregate and scrub that data
24 isn't simple, and I recognize that.

25 And of course, this kind of data is not available

1 in ISAC. No one wants data shared in a way that creates new
2 vulnerabilities, and that's in my opinion, one of the
3 reasons the regional entities were created the way they were
4 with delegated governmental authority on things like
5 mandatory assessments and enforcement authority, but without
6 certain operational requirements that are typical to other
7 government agencies like FOIA and other things.

8 What WECC shares right now, and I don't know what
9 the other regional entities do, but what WECC shares on
10 compliance is the percentage of non-compliance that are
11 self-reported versus discovered, and a high level indication
12 of cause. Sharing more than that isn't simple, and it
13 creates both risks, but it does create potential benefits,
14 and it requires consideration of all of those.

15 As has been said before in this meeting when an
16 event happens in a state, usually it's the state regulators,
17 or the Governor's office who gets the first request of
18 what's going on and what's happening. Another benefit,
19 potential benefit of more information sharing is
20 consistency. I know in Utah, most of the standards that are
21 enforced by the NERC regional entity, are also incorporated
22 by reference into state law, with jurisdiction over those
23 given to our Commission.

24 And no one wants a patchwork of inconsistent
25 state and federal enforcement of regulations, so more

1 information sharing can lead to a more consistent
2 application and understanding of these requirements. And it
3 can also help state regulators make better decisions on
4 approving costs, and cost recovery with respect to what's
5 spent on these.

6 Now I'm not suggesting a specific outcome.
7 There's a lot of more questions than answers on this
8 suggestion, but I think encouragement from FERC and NERC to
9 the regional entities to consider this, to engage in some
10 fresh evaluation of whether there's a way to aggregate data
11 that overcomes the risks with data sharing can benefit --
12 could benefit both the regional entities and the state
13 regulators.

14 As I make this suggestion I'm not sure how well
15 it's connected to this, but I can't stop thinking about a
16 tweet I read a few months ago from the American philosopher
17 Ice-T, who said, "If you loan money to a friend, be
18 prepared to lose one of them."

19 And, you know, information sharing could damage
20 the relationship between regional entities and state
21 regulators if it's not done right. It has to be done
22 properly, and so that's why I suggest a careful evaluation
23 of what can be done, what might be done, but I think there's
24 potential there. And there's potential to move the needle
25 on coordination between these entities. Thank you.

1 DR. RAAB: Chair Dutrieuille?

2 CHAIR DUTRIEUILLE: It's hard to go after that.
3 I don't have a quote. I think the essence of what you're
4 going to hear from me, we've been hearing it throughout. I
5 can say throughout today since we had a session in the
6 morning as well. But I just want to emphasize a few things.
7 So when we're talking about risk and knowing where the risks
8 are, I wanted to emphasize that it's important -- of course
9 my notes -- okay, it's important in terms of State
10 Commissions also to focus on gaining knowledge about what to
11 expect if and when a particular facility is compromised.

12 So some of the questions that we probably could
13 be asking, you know, we're looking for answers, to is do
14 utilities have reasonable, sufficient, replacement equipment
15 in inventory for recovery? I don't think we've talked much
16 about that. And that could include do they have agreements
17 in place. We talk a lot on the local level, the
18 distribution level in terms of mutual assistance
19 agreements, but this would be agreements to be borrowing
20 equipment.

21 You know, we're talking about, you know,
22 transformers and things of that nature, which is not a small
23 piece of equipment, but also on the communication side, are
24 utilities ready to ask the hard questions that, you know, in
25 terms of the incident, how long is it going to take in terms

1 of restoration? Those are some of the things that I wanted
2 to emphasize.

3 But I also want to get back to what I think we've
4 been talking about all along in terms of communication. And
5 two sides of it in terms of communication. Communication
6 between the utilities and State Commissions, and then
7 communications between FERC and the states.

8 So, with regard to communication between
9 utilities and State Commissions, the transmission owners are
10 obligated to identify the CIP 14 facilities to their system
11 operator. But they should also actively work with their
12 Commissions to develop procedures required for the
13 consideration of confidential and extraordinarily sensitive
14 information.

15 And I know we talk about that generally, every
16 state is different in terms of whatever statute they have in
17 place, and then the concerns that we want to make sure we're
18 protecting sensitive information.

19 With regard to communication, in terms of FERC
20 and state, and sharing of the information, you know, we talk
21 a lot about advocating for the buildout of transmission in
22 terms of more transmission facilities. And I just wanted to
23 make a point that I think it's crucial that when we're
24 talking about siting of these facilities, and when they
25 occur, how they occur, the affected states it should be

1 where the states are getting more of an understanding of
2 what's considered to be critical.

3 I think that's important in the planning process
4 and things of that nature, and I just wanted to emphasize
5 that. And there's still you have to look at it in terms of
6 protecting critical information, but still as we can talk
7 back and forth and share information, I think it's the
8 knowledge of what's considered to be critical as part of
9 that communication. Thank you.

10 DR. RAAB: Commissioner Houck?

11 COMMISSIONER HOUCK: Can you hear me? Okay.
12 Thank you. And consistent with the comments of my
13 colleagues I agree with the comments that they made on this
14 topic. And as we heard earlier today from our presenters,
15 the nature of physical security presents the challenge of a
16 static infrastructure being threatened by a disaggregated
17 group of adversaries, and the dynamic set-up methods that
18 change much faster than infrastructure changes.

19 We need to take a holistic approach that we
20 deliberate, and deliberate on efforts to enhance the
21 physical security of electric infrastructure. Before
22 formulating solutions, we need to understand the danger we
23 as a nation are mitigating against. And as a state we can
24 work with our partners, to define this, but no individual
25 state has the resources or capability to establish a common

1 understanding of the threat landscape from a national
2 perspective across the nation.

3 We should develop a threat model that clearly
4 articulates the threats faced by investor owned utilities
5 across the country, and this would establish a common
6 problem set based on a common understanding of the threat.
7 This threat analysis will allow for a more refined
8 delineation of respective roles and responsibilities for
9 federal, state and local agencies, for enhanced coordination
10 of physical security efforts, and this would also assist in
11 any formulation of regional groups.

12 After a threat model has been established,
13 stakeholders have been identified, and roles and
14 responsibilities have been defined, we can jointly apply
15 short-term physical infrastructure measures, mitigation
16 efforts, stock-piling requirements, and potentially
17 long-term changes to infrastructure to make it more
18 resilient.

19 As part of such efforts California recommends
20 leveraging existing analysis and research that's been
21 developed by various federal agencies and the National Labs.
22 This includes research and analysis of infrastructure,
23 response frameworks, and resilience initiatives.

24 Without these steps our efforts for risk become
25 more aspirational than effective. And in regards to the

1 information sharing, there are currently mechanisms for
2 information sharing between investor-owned utilities, states
3 and federal departments. However, information sharing
4 between all stakeholders is not as fluid as it needs to be
5 to maintain a common understanding of the changing threat
6 landscape.

7 The current mechanisms need to be maintained and
8 enhanced by establishing and re-establishing appropriate
9 thresholds for information sharing between partners within
10 an environment of trust.

11 To improve resiliency, it's essential that this
12 information be exchanged not only between state and federal
13 level threat centers, but also among the investor owned
14 utilities, and that the right level of information is shared
15 to allow for better analysis of the threat landscape.

16 Regular and routine sharing of information, such
17 as best practices related to safety and security procedures,
18 response to events, and short and long-term recovery can
19 enhance local, state and regional security overall. This is
20 a highly technical, and collaborative endeavor to achieve
21 these outcomes. NARUC could facilitate a physical security
22 preparedness initiative to provide stakeholders with
23 information they need to assess and respond to evolving
24 threats.

25 And one model that could be considered is the

1 CAPS model, the cybersecurity and the solar projects that
2 NARUC has convened, which leverages state, federal and
3 private sector expertise to identify model programs and
4 actions for states to take in partnership with utilities.

5 This could be implemented similar to the
6 initiative for the physical security that NARUC has
7 convened, state led advisory group and facilitate dialogue
8 with IOUs and physical security experts to provide education
9 tools, and access to technical assistance.

10 This initiative could develop actionable,
11 physical security strategies, and a roadmap, as well as
12 create stronger public, private partnerships in intra and
13 interstate cooperation. And the goal would be for the
14 federal government and states to work with IOUs to establish
15 the appropriate processes, organizational components, and
16 information thresholds that work best for their operational
17 needs, and limitations concerning the sharing and
18 protection of sensitive, critical infrastructure and
19 incident information. Thank you.

20 DR. RAAB: Thank you. Commissioner Christie?

21 COMMISSIONER CHRISTIE: This is sort of the
22 question I asked Jim Robb earlier, so I guess I jumped the
23 gun. But he said that the question of prioritization is
24 addressed in CIP 14, and I wish he were still here because
25 I'd like to follow-up and ask him what about the

1 prioritization process, and the issues that these questions
2 address, what is not covered in CIP 14?

3 Who ultimately makes the decision about what
4 facility is going to get the ballistic curtain, or going to
5 get the high def camera? And I don't know whether CIP 14
6 actually says who makes that final call or not, so I wish
7 Jim was still here. I think that's a big open question is
8 where does that final call get made about which substation
9 gets that ballistic curtain, or that high def camera, or
10 whatever other measure it is.

11 The second thing I was going to mention too,
12 better here than nowhere else, but ballistic curtains, high
13 def cameras, these are expensive items. If I was still a
14 state regulator I'd be scared to death about what the cost
15 is going to be, because this is going to flow right through
16 into retail rates.

17 It's necessary. We're obviously going to have
18 to do it. But I think the prioritization is critically
19 important to make sure that -- because you can't do it
20 everywhere, it would just be astronomical. So I think this
21 prioritization process about deciding which ones get it, is
22 critically important to keep, you know, just an exorbitant
23 amount of money from flowing right through into retail
24 bills.

25 And these are transmission assets, so you're

1 probably talking formula rates to start with. You're not
2 even talking state distribution rates. You're talking
3 formula rates. So I hope this prioritization issue
4 continues to get more attention, and again, I wish Jim were
5 here to tell us about where's the gap in CIP 14 about who
6 makes that decision. It's really important to get that
7 right.

8 DR. RAAB: So others want to jump in on this
9 topic, either what you've heard, or other thoughts that you
10 want to add. Thank you. Chair Scripps?

11 CHAIR SCRIPPS: I'll do my best. And I was going
12 to maybe get one sentence in my comments on the next
13 question, but I think it was I think directly in response to
14 the question that Commissioner Christie brought up. Because
15 my understanding is that the ultimate decider of who makes
16 the -- the ultimate decider is the transmission owner.

17 And that plan that they put forward has to have
18 -- be reviewed by a third party, but the ultimate decision
19 maker in this is the transmission owner. And it's one of
20 the reasons that I think some level of state oversight on
21 CIP compliance would be a benefit. I'm not sure that we
22 could sort of require them to do something more or less than
23 what they're doing.

24 But to be able to raise the question of is this
25 the right solution for the problem that's been identified,

1 as opposed to just the transmission owner saying I think I
2 need the ballistic curtain, and the third party reviewing
3 saying yeah, I think that's right.

4 COMMISSIONER CHRISTIE: Well that's a very
5 important point because I mean if there's no review, you
6 know, when you start talking about let's take high def
7 cameras or ballistic curtains. I mean are they going to be
8 treated as capitalization items with an ROE, or are they
9 going to be treated as O and M? That's a huge issue in
10 terms of cost. Well who decides that?

11 Do they just come to FERC with formula rates and
12 say we decided to capitalize it? I mean someone should be
13 looking at that. And personally, I'd rather have state
14 regulators do it, but somebody needs to do it.

15 DR. RAAB: Commissioner French?

16 COMMISSIONER FRENCH: I maybe have a little
17 different -- maybe I understood your question a little
18 differently. What I thought Mr. Robb was communicating was
19 CIP 14 is really a ranking system, or a system to determine
20 which facilities are critical enough to need this compliance
21 plan.

22 And I think, you know, I think he threw out the
23 question, and others have thrown out the question of have we
24 set that threshold at the right amount because he mentioned
25 that some of the facilities, I think for instance, in North

1 Carolina, those weren't CIP 14 facilities.

2 And so I think the question is out there, is that
3 threshold set at the appropriate level? That's a policy
4 decision, I believe ultimately, you know, within FERC's
5 jurisdiction as you work with NERC on that review. So that
6 would be my first thought. Second thought is I would just
7 want to completely agree with you on, you know, the cost of
8 new technologies.

9 And I think it's obvious my focus is on how do we
10 cost-effectively look at the topology of the current grid
11 and make sure we don't have targets. That we don't have --
12 we have as few critical facilities as possible that require
13 those super expensive upgrades, because we just can't do
14 that at 75,000 different substations, so I thought that was
15 a good point.

16 DR. RAAB: Commissioner Duffley?

17 COMMISSIONER DUFFLEY: So risks to the bulk
18 electric system are going to be different from risks to
19 localized systems, and so the state may need to be involved
20 when we're dealing with the localized, and where there won't
21 be cascading outages on the bulk electric system. So it
22 could be that there may be different standards based upon if
23 there's risk to cascading outages, or if it's just going to
24 have a local result.

25 DR. RAAB: Great. Anybody want to add anything

1 else? We'll move to our last question. Okay. So the last
2 question is what other changes should FERC or NERC,
3 Congress, the States consider, including enhanced
4 requirements and minimum standards, new expanded funding
5 sources, to reduce the risks of physical attacks on the
6 transmission system?

7 We touched on some of these, but not all of them.
8 Any other thoughts that you have? And we'll start with
9 Commissioner Christie, and Commissioner Duffley, and then
10 Chair Scripps yeah.

11 COMMISSIONER CHRISTIE: In terms of funding I
12 would urge NARUC to take a look at -- I've mentioned this
13 before, there's billions of dollars in the infrastructure
14 legislation that Congress passed for grid hardening. This
15 would be a good use for it to defray the costs to consumers.

16 So I think NARUC maybe ought to look at asking
17 the DOE to dedicate some of that money to help to defray
18 some of the cost of some of this grid hardening, which we
19 know we're going to have to do to keep it out of consumers'
20 bills.

21 DR. RAAB: Commissioner Duffley?

22 COMMISSIONER CHRISTIE: No.

23 DR. RAAB: I think you need to borrow a neighbor.

24 COMMISSIONER DUFFLEY: Now we're good.

25 COMMISSIONER CHRISTIE: Only one microphone

1 allowed at a time.

2 COMMISSIONER DUFFLEY: One microphone. You're
3 trying to prospect to others.

4 COMMISSIONER CHRISTIE: It's all yours Kim.

5 COMMISSIONER DUFFLEY: So the result of being one
6 of the last speakers, most of the salient points have been
7 made, so I'm going to keep my comments short, and maybe
8 reiterate a few. We currently have established
9 communication and coordination methods such as E-ISAC and
10 the State Emergency Management Centers that every state has,
11 and so providing more resources to these centers could
12 enhance the communications as well as the analysis of the
13 information that's being provided.

14 We also have heard today about continued
15 coordination with local law enforcement, and I fully agree
16 with that. And then what are states doing? So currently
17 what's being done in several states is they have introduced
18 bills to increase the penalties for infrastructure crimes,
19 and that should enhance deterrence.

20 CHAIR SCRIPPS: I agree with Commissioner
21 Duffley, most everything's been said. When Jim Robb was
22 talking earlier, he posed the question on how our physical
23 security approaches should balance between protection
24 measures and measures focused on restoration and recovery,
25 and I just want to offer maybe a couple thoughts on each

1 side of that equation.

2 On protection and prevention it's probably not a
3 surprise given the questions I was asking Mr. Robb, but it's
4 my belief that in addition to the process based approach
5 that makes up the core of the CIP standards, we do actually
6 need to include a minimum set of physical security
7 mitigation measures.

8 And I think there's plenty of room for agreement
9 here. The vast majority of facilities already have things
10 like standard gauge fences, locks, some degree of
11 surveillance, visual obstruction elements like fence
12 netting, et cetera. And it's simply codifying a lot of what
13 already exists.

14 And then as we gain experience, and better
15 understanding of the evolving threat environment, perhaps
16 moving that floor up over time. But I am much more
17 comfortable about having a conversation about what are the
18 right level of minimum standards, and which of those are
19 appropriate, than trying to explain why we don't actually
20 have a set of minimum standards within the CIP framework, as
21 these incidents continue to accelerate.

22 And I want to be really clear. This is in
23 addition to, not instead of. I think the process based
24 framework is the right one broadly because I do think there
25 are significant and material differences based on

1 population, based on who's connected to the substation, et
2 cetera.

3 But having a minimum set of physical security
4 mitigation measures I think would go a long way. On the
5 other side of the coin on recovery and restoration two
6 thoughts, and some of this was already previews by
7 Commissioner Brown Dutrieuille, as usual, but in March 2017,
8 responding to Congressional directives contained in the
9 Fixing America's Surface Transportation, or FAST Act, U.S.
10 DOE published a report on the concept of a strategic
11 transformer reserve. And there's been a fair amount of
12 progress made since then. Edison Electric Institute has two
13 initiatives, the Spare Transformer Equipment Program, or
14 STEP, and Spare Connect.

15 The North American Transmission Forum's Regional
16 Equipment Sharing for Transmission Restoration, or RESTORE
17 Program, and Grid Assurance, which I believe is a spin-off
18 from AEP, which offers a subscription model, are all good
19 and important steps in the right direction.

20 But I think that more is needed, particularly
21 given the challenges around supply chain issues. Because to
22 date as far as I know we don't yet have the equivalent of
23 what exists in the nuclear industry for example, with an
24 emergency equipment repository, which is an NRC initiated
25 effort in the wake of a Fukushima event, where today we have

1 three equipment depots that are strategically located, and
2 cover the whole of the U.S. nuclear fleet with standard
3 delivery times, so that restoration, or getting new
4 equipment onsite to any one of the nuclear reactors across
5 the country can be made in a timely effort.

6 So, expanding on some of the efforts from EEI and
7 the transmission forum, and some of the private sector
8 efforts. But to make sure that there aren't gaps in the
9 system in terms of some sort of shared response. And then
10 finally, this was highlighted I think most eloquently by
11 Commissioner French as usual, talking about the advantages
12 of a decentralized system with redundancy, and that that's a
13 real strength.

14 Also noted by Mr. Robb talking about the small
15 number of substations that are designated as critical, and
16 that that number should continue to decline through
17 additional redundancy, and then Mr. Kumar's point that as we
18 continue to build the system of the future, trying to build
19 in resilience as we go is important.

20 But oddly, and maybe paradoxically, but I also
21 think truly the most cost-effective long-term result may be
22 redundancy throughout the system, adding transmission,
23 looping interconnections, the development of micro grids, et
24 cetera, to reduce the impact of successful events, that they
25 become less and less critical the more redundancy that we

1 have.

2 This also has the benefit of mitigating all
3 hazards in a way that fencing or armoring do not, with the
4 climate based challenges that we're facing that have been
5 raised, as well as some of the ballistic incidents, as well
6 as the additional benefits of expanding transmission, even
7 beyond addressing physical security concerns.

8 So looking at how we add redundancy through
9 transmission expansion, may be the best and most
10 cost-effective, long-term approach to dealing with physical
11 security threats, and one that also has a host of additional
12 benefits as well.

13 DR. RAAB: The floor is open for your reactions,
14 additions, as we're getting near the end. Yeah,
15 Commissioner Allen then Chair Stanek.

16 COMMISSIONER ALLEN: Yeah. I just want to throw
17 a little support behind what Chair Scripps had mentioned
18 about physical standards. I think physical CIP standards,
19 or minimum standards, for physical security threats, or
20 other hazards to the physical transmission system make sense
21 to me.

22 I think you need to be considering flexibility to
23 differentiate by the kind of critical nature of certain
24 assets, or potentially provide flexibility at either a
25 state, regional, or through transmission operator level. I

1 think that then begs the question of what is in the
2 conversation that I've been having earlier, what is the kind
3 of sensible analytic framework for figuring out what those
4 minimum standards are.

5 And harkening back to Commissioner Christie
6 leveraging the federal funds, absolutely.

7 CHAIR STANEK: Following up from Commissioner
8 Duffley, the states may need to take action on their own to
9 increase the penalties in state law, in terms of any attacks
10 on an energy facility. I'm looking at the criminal
11 complaint, the indictment that occurred yesterday in the
12 U.S. District Court of Maryland, and it's being charged
13 under the crime of conspiracy to destroy an energy
14 facility, that's 18 U.S. Code Section 1366.

15 The penalty is not more, not more, than 20 years
16 behind bars. So it could be a slap on the wrist. They're
17 in and out in one year. That's the federal law, so I would
18 implore Congress to revisit this statute. But at the same
19 time the states have the ability to pass their own laws to
20 make it not a minimum, but a floor, not a ceiling.

21 DR. RAAB: Anybody else want to add? Okay. So
22 we've touched on many things briefly, but we've touched on
23 them from better information sharing, and better information
24 channels to thinking about more, maybe standardized risk
25 assessment methodologies, to, should there be minimum

1 standards for risk mitigation to, in the longer term,
2 planning and developing, consistent with what we've been
3 thinking before, more redundant system planning for just
4 resilience generally.

5 Thinking about leveraging federal funds to assist
6 with this, increasing penalties as a way of deterrence, and
7 that's the beginning of a list of I think a lot of good
8 things that we touched on. Obviously, the next step is at
9 least, big step, is there will be a report filed by NERC on
10 what they're recommending, what their analysis of how things
11 have changed, and what might be considered.

12 I think you got a little bit of foreshadowing of
13 the things that NERC is thinking about, or wrestling with,
14 and so I think we'll all be -- you will all be in a much
15 better place now to take a look at that, and see what this
16 list and other things are in there, or not in there, and
17 then to continue the conversation either within the Task
18 Force or other ways. So I will turn it back to our
19 illustrious Co-Chairs.

20 CHAIR STANEK: Thank you Dr. Raab. This was a
21 very enlightening meeting that we had today. This is the
22 first meeting where the State Commissioners weren't
23 attempting to actually lobby our FERC colleagues in terms of
24 a rule, so that reduced the temperature just a bit.

25 But I do believe what Director Kumar stated that

1 we do need a whole of government approach. We see these
2 threats not only on the horizon, they're on the table today,
3 and for one reason or another they're multiplying. We need
4 to be proactive, but as Chair Pridemore and Commissioner
5 Houck mentioned, we need to be mindful as well of the costs.

6 Ultimately, ratepayers are going to be paying for
7 all of these proactive measures, but at this time we do have
8 to do a cost benefit assessment, and a risk-based approach.
9 So I think today's discussion what we'll take back it was a
10 fact-finding mission.

11 We'll need to work with our other federal
12 colleagues not at this table, DOE, law enforcement, federal
13 agencies that we haven't previously worked with before in
14 order to get ahead of this, and to prepare for the next
15 event because unfortunately there probably will be more
16 events that will affect our states and the country in the
17 coming years.

18 So thank you to my colleagues for a very
19 productive conversation today.

20 CHAIRMAN PHILLIPS: Thank you Chair Stanek.
21 Excellent meeting everyone. I thank you for your thoughtful
22 comments. There was no lobbying today perhaps, but what you
23 said will inform what FERC does going forward. And we
24 appreciate that.

25 Very quickly I want to thank all the staff that

1 pulled this together, the NARUC team, you know, the folks
2 that ran the AV. Everyone who participated today. Give
3 them a round everybody. I think we're contractually
4 obligated to say Michelle Malloy's name every time we have a
5 meeting, and I want to make sure I do that.

6 The next meeting -- that's right, comp my room
7 next time Mr. Christie. The next meeting will be in Austin
8 at the NARUC summer meeting. That's the plan. Chair Stanek
9 and I, we already started thinking of creative ways for this
10 group to evolve, and so we welcome any ideas that you might
11 have to make these meetings even more interactive and
12 better.

13 So with that, that's all that I have. We are
14 adjourned. Thank you.

15 (Whereupon the Joint Federal-State Task Force on
16 Electric Transmission was adjourned at 3:51 p.m.)

17

18

19

20

21

22

23

24

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CERTIFICATE OF OFFICIAL REPORTER

This is to certify that the attached proceeding
before the FEDERAL ENERGY REGULATORY COMMISSION in the
Matter of:

Name of Proceeding:

Sixth Meeting of the Joint Federal-State Task
Force on Electric Transmission

Docket No.: AD21-15-000

Place: Virtual and in person at the Washington
Renaissance Hotel in Washington, D.C.

Date: Wednesday, February 15, 2023

were held as herein appears, and that this is the original
transcript thereof for the file of the Federal Energy
Regulatory Commission, and is a full correct transcription
of the proceedings.

Charles Hardy
Official Reporter

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America)
v.)
Sarah Beth CLENDANIEL)
and)
Brandon Clint RUSSELL)

Case No. 23-mj-00401-MJM

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 12 through February 2, 2023 in the county of Baltimore in the District of Maryland, the defendant(s) violated:

Code Section 18 U.S.C. 1366 Offense Description Conspiracy to Destroy an Energy Facility

This criminal complaint is based on these facts:

See affidavit.

Continued on the attached sheet.

Patrick W. Straub

Complainant's signature

Patrick W. Straub, FBI, Special Agent

Printed name and title

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: 2 2 23

[Signature]

Judge's signature



City and state: Baltimore, Maryland

Hon. Matthew J. Maddox, U.S Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Special Agent Patrick W. Straub of the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. This affidavit is being submitted in support of a Criminal Complaint charging **SARAH BETH CLENDANIEL** and **BRANDON CLINT RUSSELL** with conspiracy to damage an energy facility, in violation of 18 U.S.C. § 1366(a) (Destruction of Energy Facility).

PROBABLE CAUSE

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”). As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. I have been a Special Agent with the FBI since January 2005. I am assigned to the Joint Terrorism Task Force (“JTTF”) in the FBI Baltimore Division. The majority of my career has been devoted to investigating, managing, and supporting both international and domestic terrorism investigations, which often involve violations of Title 18 of the United States Code. I have assisted in the preparation of numerous search warrant applications, conducted, or participated in physical and electronic surveillance, assisted in the execution of search warrants, debriefed informants and reviewed other pertinent records. Through my training, education, and experience, I have become familiar with the efforts of persons involved in criminal activity to avoid detection by law enforcement.

BACKGROUND INFORMATION CONCERNING RUSSELL

4. In May of 2017, RUSSELL resided in Tampa, Florida with three roommates when one of them, Devon Arthurs, murdered the other two roommates. **RUSSELL** was not home at the time and was not harmed. During the ensuing response and investigation, police discovered Neo-Nazi paraphernalia, a picture of Oklahoma City bomber Timothy McVeigh, the high explosive hexamethylene triperoxide diamine (“HMTD”) and, among other items, numerous explosive precursors that belonged to **RUSSELL**. During an interview, RUSSELL admitted to subscribing to “National Socialist,” or Nazi, beliefs, that he had started his own local National Socialist Group called the “Atomwaffen,” that his roommates were members of Atomwaffen, and that he had manufactured the HMTD.

5. The Atomwaffen Division (“AWD”) is known to law enforcement to be a US-based racially or ethnically motivated violent extremist (“RMVE”) group with cells in multiple states. The group’s targets have included racial minorities, the Jewish community, the LGBTQ community, the United States Government, journalists, and critical infrastructure. AWD reportedly has international ties. Since the arrest of RUSSELL and other AWD members, the AWD has renamed itself the National Socialist Order (“NSO”).

6. Devon Arthurs was arrested and charged with murdering his two roommates. Arthurs was interviewed by law enforcement agents, and he stated that he had recently converted from Neo-Nazi beliefs to Islam. Arthurs stated that he murdered his roommates because they bullied him over being a Muslim. Arthurs said that **RUSSELL** was the leader of the Neo-Nazi group to which he and his roommates had belonged. Arthurs stated that, before he killed his roommates, they had been planning to attack U.S. infrastructure, to include power lines along

“Alligator Alley” (a nickname for the part of Interstate 75 that crosses South Florida) as well as a Florida nuclear power plant.

7. **RUSSELL** was charged with, and ultimately pleaded guilty to, possession of an unregistered destructive device, in violation of 26 U.S.C. §§ 5841 & 5861(d), and improper storage of explosive materials, in violation of 18 U.S.C. § 842(j). *See* MDFL Case No. 17-cr-00283-SCB-JSS. On January 9, 2018, **RUSSELL** was sentenced to 60 months in prison, to be followed by 3 years of supervised release. **RUSSELL** has served his sentence and is currently on supervised release.

PLOT TO ATTACK ELECTRICAL SUBSTATIONS IN MARYLAND

8. According to reporting from an FBI Confidential Human Source (“CHS-1”), since at least June 2022, the user “Homunculus” on encrypted communication application #1 (“ECA #1”) has encouraged CHS-1 to carry out attacks against critical infrastructure in furtherance of his RMVE ideology. Homunculus has specifically encouraged CHS-1 to attack electrical substations and has provided guidance on how to cause maximum damage. For example, Homunculus made statements in direct messages to CHS-1 throughout much of 2022 regarding conducting critical infrastructure attacks, including statements about sniper attacks against substations, and how conducting a small number of attacks on electrical substations could cause a “cascading failure.” On September 9, 2022, Homunculus encouraged CHS-1 to read a white supremacist publication that provided instructions on how to attack critical infrastructure, and encouraged CHS-1 to use Mylar balloons to short out a power transformer. On October 14, 2022, during a conversation about the use of Mylar balloons, Homunculus told CHS-1 that “putting holes in transformers though is the greatest thing somebody can do.”

9. On October 25, 2022, after CHS-1 had provided photographs of an electrical substation, Homunculus stated that transformers are “custom made and could take almost a year to replace if there isnt [sic] any stocked replacement which they liekly [sic] dont have.” Homunculus also sent a link to the Wikipedia page for “Cascading failure” and asked CHS-1 how cold it gets in CHS-1’s area. Homunculus stated that CHS-1 should carry out an attack “when there is greatest strain on the grid,” like “when everyone is using electricity to either heat or cool their homes.”

10. On November 5, 2022, Homunculus asked CHS-1 if it was snowing in CHS-1’s area yet and added: “i think you should wait until like a week after it starts snowing for that other thing we talked about.” CHS-1 reported that the “other thing” was a reference to an attack on an electrical substation. Homunculus also stated that the “goal is for when most people are using max electricity” and that “follow on [attacks] could lead to cascading failure costing billions of dollars.” CHS-1 replied with an emoji of a shocked rubber duck.

11. On December 3, 2022, Homunculus told CHS-1, “someone else i know in maryland...is gonna be doing same thing as you” and that this would “GREATLY amplify its effects.” During the same conversation, Homunculus confirmed he was referring to the “thing [CHS-1] sent pictures about,” a reference to the photographs of an electrical substation provided by CHS-1 in late October.

12. On January 12, 2023, CHS-1 discussed the planned substation attack and told Homunculus that CHS-1 wanted to “maximize impact” and “[w]ould love to coordinate to get multiple [substations] at the same time.” CHS-1 also alluded to the concept of cascading failure that Homunculus had explained to CHS-1 during previous conversations. Homunculus asked CHS-1 to collaborate with a Maryland-based woman to carry out the attacks. Homunculus

confirmed that the woman was 100 percent “serious and can be trusted.” Homunculus described the woman as a “felon” who “had their weapon stolen” and was struggling to obtain a new weapon. Homunculus asked CHS-1 to assist.

13. According to reporting from CHS-1, later on January 12, 2023, ECA #1 user “Nythra88” (“Nythra”) introduced herself to CHS-1, confirmed she was the individual Homunculus was referring to in the previous conversation, and stated that she lived near Baltimore. As described further below, FBI investigators have identified Nythra as Sarah Beth **CLENDANIEL**. During the conversation, which continued through January 14, 2023, Nythra informed CHS-1 that she had a terminal illness related to her kidneys and was unlikely to live more than a few months, confirmed she is a felon, and stated she had previously, but unsuccessfully, attempted to obtain a rifle. Nythra requested that CHS-1 purchase a rifle for her and that she wanted to “accomplish something worthwhile” before her death, and wanted the rifle “within the next couple of weeks” to “accomplish as much as possible before June, at the latest.” Nythra provided CHS-1 with the encrypted communication application #2 (“ECA #2”) account (@kali1889) and suggested future communication occur there, via voice, or in person.

14. On or about January 18, 2023, CHS-1 engaged in a recorded voice discussion using ECA #2 with @kali1889 (“Kali”). During that conversation, Kali told CHS-1 that she had already identified a few potential locations to target in her attack, including one just across the Delaware state line (with Maryland), in a location that is “literally like a life artery” and would “definitely cut out a lot of shit.” Kali confided that she had just obtained her driver’s license “today” and was not that comfortable driving yet, so CHS-1 stated that CHS-1 would have to be the “driver” and Kali would have to be the “shooter” in the attack. Kali confirmed that she was “determined to do this” and stated she would have done something earlier on her own if she had not lost her rifle “a

few months ago.” Kali told CHS-1 that she had an “eotech with a 4 times magnifier,” which CHS-1 assessed to be a rifle optic. Kali told CHS-1 that she had previously tried to obtain a rifle, a Smith & Wesson M&P 10 Sport, but that had fallen through. Kali told CHS-1 that, if CHS-1 provided her a rifle, CHS-1 should report the rifle as stolen and she would then file off the serial number. Kali emphasized that her time frame for the attack was “no longer than a month.”

15. The above call on ECA #2 experienced technical difficulties, so the recorded voice conversation continued shortly thereafter on ECA #1. During the ECA #1 voice call, CHS-1 and Nythra continued to discuss the specifics of the desired rifle and agreed that Nythra would send CHS-1 a “wish list.” Nythra acknowledged that whatever type of firearms she possessed would be “illegal.” Nythra also stated that she would “really want a silencer for my Glock 9.” FBI investigators believe that Nythra’s reference to a “Glock 9” was regarding a Glock 19, which is a handgun that uses 9-millimeter ammunition. On or about January 19, 2023, Kali sent CHS-1 a wish list of items for her desired rifle that were available for online purchase at www.palmettostatearmory.com, including an “upper,” a “lower” and magazines.

16. On or about January 19, 2023, CHS-1 engaged in a recorded voice discussion with ECA #1 user Homunculus during which they spoke about CHS-1’s conversation the prior day with Nythra. Specifically, they discussed Nythra’s ability to participate in the attack due to her health problems and possibilities regarding acquiring or manufacturing a rifle for her. Homunculus advised CHS-1 that he did not think CHS-1 and Nythra needed to be together at the same location during the attack. When CHS-1 asked whether they would need to attack substations near one other in order to achieve “cascading failure,” Homunculus said it “depends.” Homunculus said he would “look at the map” and get back to CHS-1 about target facilities in a couple of days.

17. On January 21, 2023, CHS-1 exchanged encrypted messages, separately, with Kali on ECA #2 and Homunculus on ECA #1 in which they discussed in more detail the rifle and specific accessories Kali desired. The conversation with Kali extended into January 22, 2023, at which time Kali stated that she already had a “bunch of [.308] ammunition” and several magazines for a rifle. Kali later clarified that she had a “few hundred rounds of ammunition.” Kali also asked CHS-1 to provide her a “decent inner pants holster” for her “9mm” to replace her “other holster” which is a “drop leg holster” and therefore difficult to conceal.

18. On or about January 24, 2023, CHS-1 engaged in a recorded voice discussion on ECA #1 with Nythra that lasted almost two hours. During the call, they discussed, among other things, the following:

- a. Nythra previously had a semi-automatic rifle; however, in approximately October 2022, it was taken by an unnamed individual during an argument when Nythra, her son, and her nephew, were caught trespassing on the individual’s property.
- b. Nythra has threaded and non-threaded barrels for her Glock, which is functional after she purchased a new “slide” for it. Nythra physically has the Glock with her; it is not kept at her mother’s residence. Nythra further explained, “I keep it on me now, like just in case.” Nythra said she would send a picture of it to CHS-1 in the next day or two.
- c. Nythra discussed the ammunition she has, including .308 “full metal jacket” rounds, hollow point nine-millimeter rounds, and approximately 150-200 rounds of “Browning and Winchester.”

- d. Nythra has a “Tri-Star” semi-automatic shotgun with a 10-round magazine that she could use instead of the desired rifle in the “worst case scenario.”
 - e. Nythra commented that her brother has or had some “incendiary rounds” with a green tip. Although expensive, Nythra suggested: “getting that is, uh, I think especially for what we’re talking about doing, just to make sure it’s a solid thing and not just like the oil leaking out but like it’s fully damaged.”
 - f. Nythra stated that she and CHS-1 needed to use “brass catchers,” and she had thought about going to the firearms range to collect shells of different calibers, including .556, that they could spread “there” to send “them” on a wild goose chase. FBI investigators believe that Nythra was suggesting they attach devices called “brass catchers” to their rifles to collect spent shell casings during their planned attack; they would instead leave shell casings of different calibers at their attack locations, so that investigators who responded to the crime scenes could not tie the casings to the actual rifles used by Nythra and CHS-1.
 - g. Nythra was hesitant to discuss targets of the attack with “Raccoon” (another alias for Homunculus) because “he has a lot to lose.” She added: “He’s not like your average regular one of us that’s not known and that’s like a faceless unknown person . . . I try not to involve him wherever possible.” Nythra and CHS-1 discussed physically scoping out some potential attack sites during the first week of February.
 - h. Nythra and CHS-1 further discussed Nythra’s desired rifle for the attack.
19. On or about January 26, 2023, CHS-1 and Homunculus exchanged direct

messages on ECA #1 during which CHS-1 advised he/she had tentatively decided to buy a “pre-made” rifle for Nythra/Kali instead of 3D printing one, and Homunculus replied: “okay sounds good . . . everything else is fine too ;)” When CHS-1 asked if Homunculus was referring to “location”, Homunculus simply replied “yes don’t worry.” CHS-1 stated: “Perfect. That’s the part that I haven’t really done anything on,” to which Homunculus again replied: “yea don’t worry.” Based on the context and previous messages, CHS-1 knows that Homunculus understood that “location” meant the specific substation that would be targeted.

20. On or about January 29, 2023, CHS-1 received a message on ECA #2 from Kali in which Kali stated it “would really be ideal, for us both to have 30 round mags. Especially for what we’re doing.” She asked CHS-1 to “please get us each like, 4 of them. For what I’m hoping to do, we will need them. If we can pull off what I’m hoping... this would be legendary. This is MAJOR tier, and definitely doable.”

21. On or about January 29, 2023, Kali sent CHS-1 via ECA #2 a link to the publicly available webpage “Open Infrastructure Map” (<https://openinframap.org>) and instructed CHS-1 to “look at Baltimore and see if you can figure out what I want to do.” She also stated she wanted “to try to do 5 in one day.” CHS reported that he/she understands that to mean Nythra seeks to attack five electrical substations on the same day.

22. On or about January 29, 2023, Nythra told CHS-1 during a recorded voice conversation on ECA #1 that the five substations she planned to target included: “Norrisville, Reisterstown, and Perry Hall.” Nythra described how there was a “ring” around Baltimore and if they hit a number of them all in the same day, they “would completely destroy this whole city.” Nythra added that they needed to “destroy those cores, not just leak the oil...” and that a “good four or five shots through the center of them . . . should make that happen.” She added:

“It would probably permanently completely lay this city to waste if we could do that successfully.” CHS-1 asked if it would accomplish a “cascading failure” and Nythra replied: “Yes . . . probably” and that the attack targets are all “major ones.” Nythra added that the most difficult target that they would have to do together has “fire walls on three sides.”

23. Nythra also sent CHS-1 five links to the “Open Infrastructure Map,” which is the same website previously disseminated by Homunculus when discussing infrastructure attacks (discussed above), showing the locations of five specific electrical substations in Maryland. Three of the five substations appear to be located near the towns of Norrisville, Reisterstown, and Perry Hall. The remaining two substations are in the vicinity of Baltimore City, MD. CHS-1 reported that he/she understands these five links to show the targets of Nythra’s planned attack. The FBI reviewed the links provided by Nythra, located the substations/areas on Google Maps, and physically visited and photographed each site. Each location is a BGE substation with significant infrastructure. Based on my training and experience, and via open source research, I know that BGE is an energy company that utilizes substations, like the five targeted sites, to produce, convert, transform, regulate and distribute energy.

24. On or about January 31, 2023, CHS-1 and Homunculus communicated via encrypted chat on ECA #1. CHS-1 told Homunculus that he/she had “read about a few attempt [sic] recently that didn’t have much effect, so I want to make sure it’s done right.” Homunculus replied “Yea, it has been studied . . . So don’t fret.” CHS-1 asked about “These specific 5?” to which Homunculus replied: “Look at the map dude.” CHS-1 responded: “So that’s the part I don’t get. What’s with the one all the way up by Pennsylvania? Does that have something to do with the cascading?” Homunculus replied: “Watch this video” and provided a YouTube link to a video captioned “Grid vs. Gunfire” that discussed “What Really Happened with the Substation

Attack in North Carolina.” After watching the video, CHS-1 commented that he/she is looking at the map and “I think I get it . . . But I only see four lines. Not fully getting the fifth. Is the one up north to stop rerouting? You know the one I’m talking about?” Homunculus replied: “Yrs [sic]... It’s a hard one though . . . Look at it from google maps.” After indicating he/she had pulled the location up on the map, CHS-1 replied “It looks like it’s in a pretty rural area . . . Good road access . . . Wooded areas . . . I would like it to be closer to a major highway, but that has its ups and downs. Homunculus replied: “Yea . . . Hard part is they have 3 sided firewalls . . . Look at them.” CHS-1 replied: “Oh shit. Yea this is that one. Our friend mentioned that one did but she didn’t say which one.”

25. Based on my training and experience, as well my knowledge of the facts in this investigation, I understand the above chat between CHS-1 and Homunculus to be a discussion of the five substations that Nythra had previously identified as targets for her attack with CHS-1. One of the five substations identified by Nythra is in a rural area of Maryland near the Pennsylvania border. In addition, Nythra described a substation as being surrounded by “fire walls” on three sides, which is the same language Homunculus used to describe the facility near Pennsylvania on January 31, 2023. As a result, I submit that there is probable cause to believe that Nythra and Homunculus discussed potential target locations and jointly selected the five attack targets that Nythra shared with CHS-1.

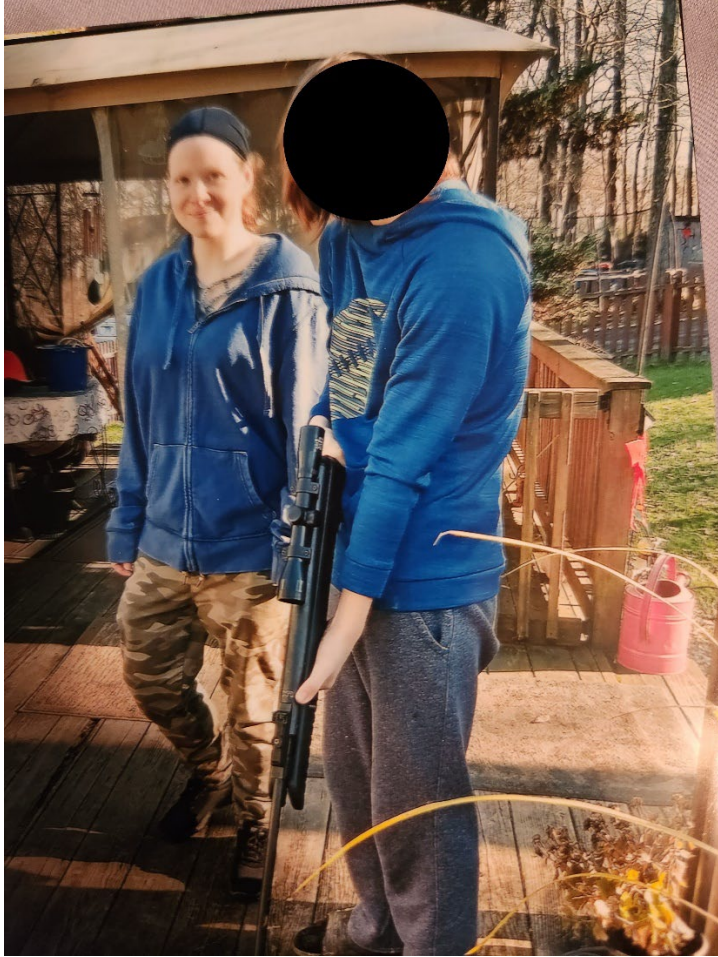
26. The FBI received records from Google on January 30, 2023, and January 31, 2023, pursuant to a search warrant targeting accounts used by **CLENDANIEL**.¹ A preliminary review of a portion of these records revealed additional evidence of **CLENDANIEL**’s criminal activities and her identity as “Kali1889” and “Nythra88. For instance, the records included

¹ The search warrant was issued by United States Magistrate Judge for the District of Maryland A. David Copperthite on January 27, 2023. *See* No. ADC- 23-349.

several photographs of ammunition, an “eotech” firearm sighting accessory, and a woman physically resembling **CLENDANIEL** in possession of or with easy access to firearms or firearm accessories, including one shown below with what appears to be a minor holding a firearm.² One photograph depicted a woman believed to be **CLENDANIEL** wearing tactical gear containing a swastika, holding a rifle and with a pistol in a drop holster on her left leg:



² I have compared the photographs to **CLENDANIEL**'s Maryland Department of Motor Vehicles photograph and believe them to be photographs of the same person.



27. The Google records also contained screenshots of a document that states that it is not a manifesto; however, the FBI assesses that it contains many aspects that would be included in a manifesto. The document starts: “If this is being posted online, I can only hope that some of

my plans were at least partially successful.” The document references Kaczynski, Brevic, Hitler³ and others while stating that “I would sacrifice ****everything**** for my people to just have a chance for our cause to succeed.” The document later states: “Unfortunately, I have very little experience with firearms. But once I get my license, I hope to get at least a couple hours of practice in . . . What a shame I don’t have a rifle yet. This storm would be the perfect time to hit some substations and knock out power.”⁴

***CLENDANIEL** is “Nythra88” on ECA #1 and “@kali1889” on ECA #2*

28. The FBI has been aware of **CLENDANIEL**’s relationship with the user of Homunculus, identified as **RUSSELL** (explained below at paragraphs 33 - 36) since at least 2018 when they were corresponding with each other while they were both incarcerated in separate facilities. In or about November 2022, if not earlier, the FBI had tentatively identified the user of the online monikers “Kali” and “Nythra88” as **CLENDANIEL**. This identification is further corroborated by the above-described voice conversations, as more fully explained below.

29. Specifically, Nythra/Kali disclosed certain details about her life to CHS-1 during the voice conversations on January 18, 2023, that correspond with **CLENDANIEL**. For instance, she stated that her mother lives in North East, Maryland but that she lives near Baltimore with a roommate. Second, Nythra/Kali stated that she had just obtained her driver’s license “today” Finally, Nythra/Kali disclosed that her prior felony conviction was for armed robbery of a convenience store with a “machete,” which she had committed while under the influence of

³ The FBI understands these to be references to Ted Kaczynski, aka the Unabomber, who was arrested in 1996 for a series of mail bombings in the United States; to Anders Breivik, who was convicted in 2012 in the Netherlands for committing terrorist attacks; and to Adolph Hitler.

⁴ Based on the fact that **CLENDANIEL** only recently obtained a driver’s license, I believe that the reference to “license” is a reference to her driver’s license.

drugs.

30. A review of Maryland Motor Vehicle Administration (MD MVA) records revealed that **CLENDANIEL**'s Maryland driver's license was issued on January 18, 2023, and her address was listed as an address known to the FBI in North East, Maryland, where her mother currently resides (hereinafter, "Subject Address 1"). A review of **CLENDANIEL**'s criminal history reflects a 2006 arrest for numerous offenses, including armed robbery, that resulted in a felony robbery conviction. **CLENDANIEL** was sentenced for this incident in approximately December 2006 to five years of imprisonment with two years suspended. The FBI reviewed a police report from this May 2006 incident, and the report indicated that **CLENDANIEL** had been arrested for her involvement in a robbery at a convenience store, during which she wielded a "large butcher knife." At the time of her arrest, officers observed "track marks, cuts and infections on both" of her arms.

31. Review of open source databases revealed that a woman believed to be **CLENDANIEL**'s mother, 72 years old, currently resides at Subject Address 1 in North East, Maryland, in Cecil County. Police reports previously reviewed by the FBI revealed that, on September 13, 2022, the resident at a different address known to the FBI in Catonsville, Maryland (hereinafter, "Subject Address 2"), had reported that **CLENDANIEL**, who was his "girlfriend," had temporarily gone missing and he provided a telephone number for **CLENDANIEL** that ended in -0728. Catonsville, Maryland is in Baltimore County and is physically located close to the city of Baltimore. The FBI reviewed information on or about January 20, 2023, from the state of Maryland regarding **CLENDANIEL**'s probation status. This information reflected that **CLENDANIEL**'s most recent contact with her probation officer was January 13, 2023, during which **CLENDANIEL** advised she was still dealing with kidney

disease. Her listed phone numbers were a phone number ending in -6453 and the same phone number ending in -0728 referenced above. Her address was listed as Subject Address 2, where she lives with her “friend.”

32. Based on all of the above, I submit that there is probable cause to believe **CLENDANIEL** is “Kali1889” and “Nythra88.”

***RUSSELL** is “Homunculus” on ECA #1 and Uses the Online Moniker “Raccoon”*

33. An FBI employee who listened to **RUSSELL**’s recorded phone calls while he was incarcerated has also listened to the recorded voice conversations between CHS-1 and Homunculus. That FBI employee believes that Homunculus and **RUSSELL** are the same person based on a voice comparison.

34. In addition, among the records obtained from Google pursuant to the search warrant are photographs of a cell phone screen displaying text messages between “Raccoon” and “Irkalla.” In the messages, Raccoon refers to Irkalla on multiple occasions as “Kali,” and, on one occasion, Irkalla refers to Raccoon as “Brandon.” In that same conversation, the two discussed having kids together, and mentioned “warfare” and “illegal things.” Raccoon stated that “going to prison was worth it because I might not have met you otherwise.”

35. In a message on ECA #1 dated July 2, 2022, Homunculus stated that “yesterday,” *i.e.*, July 1, was Brandon Russell’s birthday. Criminal history records for **RUSSELL** indicate that **RUSSELL**’s birthday is July 1. Based on the FBI’s review of these messages, it appears that Homunculus was stating in the ECA #1 messages that he was, in fact, **RUSSELL**.

36. As previously discussed at paragraph 28, the FBI has been aware of **CLENDANIEL**’s association with **RUSSELL** since 2018 and knows their relationship has persisted beyond their time in prison. For example, according to records obtained from Amazon,

CLENDANIEL's Amazon account was used to purchase items that were shipped, or scheduled to be shipped, to **RUSSELL** at his known residential address with **RUSSELL** in Orlando, Florida.⁵ One such purchase was in May 2022, and another was in August 2022. The purchase for and shipment to **RUSSELL** in May 2022 was for a 34-piece "Professional Pocket Picking Hand Tool" set that is for "Hasp Storage, Fence, Gate, Gym, Locker, Sports Locker." It is also worth noting that **CLENDANIEL** purchased the same exact item for herself, on the same day, but the order quantity was listed as "0" and the records suggest that the product was never shipped.

Conclusion

37. Based on the above information, I believe probable cause exists to support the issuance of a Criminal Complaint charging **SARAH BETH CLENDANIEL** and **BRANDON**

⁵ Bureau of Prisons records reflect that location as **RUSSELL**'s address as of the time of his release from prison in 2021. In addition, FBI personnel conducting physical surveillance have observed **RUSSELL** coming and going from that address as recently December 22, 2022.

CLINT RUSSELL with conspiracy to damage an energy facility, in violation of 18 U.S.C. § 1366(a) (Destruction of Energy Facility).

Respectfully submitted,



Patrick W. Straub, Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 2nd day of February, 2023.



THE HONORABLE MATTHEW J. MADDOX
UNITED STATES MAGISTRATE JUDGE

electricity, in an amount exceeding or which would have exceeded \$100,000, and to cause a significant interruption and impairment of a function of an energy facility.

18 U.S.C. § 1366(a)

FORFEITURE NOTICE

1. Pursuant to Rule 32.2, Fed. R. Crim. P., notice is hereby given to the defendants that the United States will seek forfeiture as part of any sentence in accordance with 18 U.S.C. § 981(a)(1)(C) and (G), and 28 U.S.C. § 2461(c), as a result of any defendant's conviction under this Indictment.

2. Upon conviction of the offense alleged in this Indictment, the defendants,

**SARAH BETH CLENDANIEL
and
BRANDON CLINT RUSSELL**

shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense, and pursuant to 18 U.S.C. § 981(a)(1)(G) and 28 U.S.C. § 2461(c), all assets, foreign or domestic, derived from, involved in, or used or intended to be used to commit any Federal crime of terrorism against the United States.

3. The property to be forfeited includes, but is not limited to, the following:
- a. one Kral Av Sanayi/Remimex semi-automatic 12 gauge shotgun bearing serial number KRC003624;
 - b. one P80 Glock-style handgun, gray in color with a black side, bearing no serial number or manufacturer;
 - c. 559 rounds of 9 mm ammunition;
 - d. 953 rounds of 7.62 mm ammunition; and
 - e. 77 shotgun cartridges.

Substitute Assets

4. If, as a result of any act or omission by any of the defendants, any of the property subject to forfeiture, identified above:

- a. cannot be located upon the exercise of due diligence;

- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States shall be entitled to forfeiture of substitute property pursuant to 21 U.S.C.

§ 853(p), as incorporated by 28 U.S.C. § 2461(c).

18 U.S.C. § 981(a)(1)(C), (G)

21 U.S.C. § 853(p)

28 U.S.C. § 2461(c)

A TRUE BILL:

2/14/2023

SIGNATURE REDACTED

Per person

Erek L. Barron
Erek L. Barron
United States Attorney

NERCNORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

April 14, 2023

The Honorable Kimberly D. Bose, Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

**Re: North American Electric Reliability Corporation
Docket No. RD23-2-___**

Dear Secretary Bose:

Pursuant to the December 15, 2022 order of the Federal Energy Regulatory Commission in Docket No. RD23-2-000,¹ the North American Electric Reliability Corporation (“NERC”) respectfully submits its report on its study evaluating Reliability Standard CIP-014-3. Communications concerning this filing should be directed to:

Shamai Elstein
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005
202-603-3331
shamai.elstein@nerc.net

NERC requests that the Commission accept this report in compliance with the directive in the December 15, 2022 order.

Respectfully submitted,

/s/ Shamai Elstein

Shamai Elstein
Associate General Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005

Counsel for North American Electric Reliability Corporation

¹ N. Am. Elec. Reliability Corp., 181 FERC ¶ 61,230 (2022).

1401 H Street NW, Suite 410
Washington, D.C. 20005
202-400-3000 | www.nerc.com

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System

April 14, 2023

RELIABILITY | RESILIENCE | SECURITY



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

Table of Contents

- Executive Summary 4
- Background 7
 - CIP-014 Development and History 7
 - FERC Order Directing Study of CIP-014 8
- Data Inputs 9
 - Regional Entity Subject Matter Experts 9
 - Electric Information Sharing and Analysis Center 9
 - Review of Planning Case Data 9
- Evaluation of CIP-014 Applicability Criteria 12
 - Analysis of Applicability Criteria 12
 - Voltage Inclusion Criterion 12
 - Weighting Factor Inclusion Criterion 12
 - Inclusion Criterion for Transmission Facilities Identified by Other Registered Entities 16
 - Inclusion Criterion for Transmission Facilities Meeting Nuclear Plant Interface Requirements 16
 - Impact Assessment of Recent Attacks on Applicability 16
 - Adequacy of Applicability Criteria Conclusions 17
- Evaluation of Requirement R1 Risk Assessment Adequacy 18
 - Analysis 18
 - Risk Assessment Deficiencies Caused by an Entity’s Model Decisions 18
 - Insufficient Technical Studies Including Insufficiently Documented Technical Rationale 21
 - Adequacy of Risk Assessment Criteria Conclusions 24
- Evaluation of Minimum Level of Physical Security Protections 25
 - Analysis of Physical Security Event Data 25
 - Known Limits of Event Data 25
 - Types of Physical Events 26
 - Physical Security Fundamentals 27
 - Design Basis Threat Risk Assessments 27
 - Implementation of the Risk Assessment 27
 - Adaptability by Design 28
 - Government Mandated Measures 28
 - Physical Security Threats and Purpose of CIP-014 29
 - Within the Scope of the CIP-014 Purpose 29
 - Outside the Scope of the CIP-014 Purpose 29

Establishing Minimum Level of Physical Security Protections Conclusions 30

Executive Summary

This report provides the North American Electric Reliability Corporation's ("NERC") updated evaluation of Reliability Standard CIP-014 ("CIP-014" or "Physical Security Reliability Standard"), consistent with the Federal Energy Regulatory Commission's ("FERC" or "Commission") December 15, 2022 order in Docket No. RD23-2-000 (the "December 2022 Order").¹ Due to an increase in reports of physical attacks on electric substations, the Commission issued the December 2022 Order directing NERC to evaluate the effectiveness of the Physical Security Reliability Standard in mitigating the risks to the Bulk-Power System ("BPS") associated with physical attacks.

The Commission directed NERC to evaluate whether the physical security protection requirements in NERC's Reliability Standards are adequate to address the risks associated with physical attacks on BPS Facilities. Specifically, FERC directed NERC to conduct a study evaluating the following: (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard; (2) the adequacy of the required risk assessment set forth in the Physical Security Reliability Standard; and (3) whether a minimum level of physical security protections should be required for all BPS substations and their associated primary control centers.

The purpose of the CIP-014 Reliability Standard is to "identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection."² The standard requires applicable Transmission Owners ("TOs") to perform periodic risk assessments of their applicable transmission stations and transmission substations (hereinafter collectively referred to as "substations") to identify which of their applicable substations are "critical" to BPS reliability (which, for purposes of CIP-014, is whether instability, uncontrolled separation, or Cascading would result if the substation were damaged or rendered inoperable). The TO must then perform an evaluation of the potential physical security threats and vulnerabilities of a physical attack to each of their "critical" substations and develop and implement a documented physical security plan to address those threats and vulnerabilities. Additionally, for each primary control center that operationally controls an identified substation, the applicable Transmission Operator ("TOP") must perform an evaluation of the potential physical security threats and vulnerabilities of a physical attack to that control center and develop and implement a documented physical security plan to address those threats and vulnerabilities.

As discussed within this report, NERC finds that the objective of CIP-014 appropriately focuses limited industry resources on risks to the reliable operation of the BPS associated with physical security incidents at the most critical facilities. Based on studies using available data, NERC finds that the CIP-014 Applicability criteria is meeting that objective and is broad enough to capture the subset of applicable facilities that TOs should identify as "critical" pursuant to the risks assessment mandated by Requirement R1. NERC did not find evidence that an expansion of the Applicability criteria would identify additional substations that would qualify as "critical" substations under the CIP-014 Requirement R1 risk assessment. Accordingly, at this time, NERC is not recommending expansion of the CIP-014 Applicability criteria.

NERC acknowledges, however, that supplementary data³ could show that additional substation configurations would warrant assessment under CIP-014. Accordingly, NERC plans to continue evaluating the adequacy of the Applicability criteria in meeting the objective of CIP-014. Following issuance of this report, NERC will work with FERC staff to hold a technical conference to, among other things, identify the type of substation configurations that should be studied to determine whether any additional substations should be included in the Applicability criteria. The technical conference would also help establish data needs for conducting those studies.

¹ *N. Am. Elec. Reliability Corp.*, 181 FERC ¶ 61,230 (2022) [hereinafter December 2022 Order].

² See Reliability Standard CIP-014-3 (Physical Security), Section A.3, Purpose. Reliability Standard CIP-014-3 is available at <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf>.

³ Namely, expansion plans, future year realized conditions, impacts of grid transformation, and other similar projections that alter year-to-year. These, in aggregate, could alter substation configuration.

NERC finds, however, that the language in Requirement R1 of CIP-014 should be refined to ensure that entities conduct effective risk assessments of their applicable substations. Information from ERO Enterprise Compliance Monitoring and Enforcement Program (“CMEP”) activities indicates that while the overall objective of the CIP-014 Requirement R1 risk assessment is sound, there are inconsistent approaches to performing the risk assessment. The ERO Enterprise observed that, in certain instances, registered entities failed to provide sufficient technical studies or justification for study decisions resulting in noncompliance. NERC finds that the inconsistent approach to performing the risk assessment is largely due to a lack of specificity in the requirement language as to the nature and parameters of the risk assessment. Accordingly, NERC will initiate a Reliability Standards development project to evaluate changes to CIP-014 to provide additional clarity on the risk assessment.

As discussed further below, the objective of the Reliability Standards development project would be to:

- Clarify the risk assessment methods for studying instability, uncontrolled separation, and Cascading; such as the expectations of dynamic studies to evaluate for instability.
- Clarify the case(s) used for the assessment to be tailored to the Requirement R1 in-service window and correct any discrepancies between the study period, frequency of study, and the base case a TO uses.
- Clarify the documentation, posting, and usage of known criteria to identify instability, uncontrolled separation, or Cascading as part of the risk assessment. The criteria should also include defining “inoperable” or “damaged” substations such that the intent of the risk assessment is clear.
- Clarify the risk assessment to account for adjacent substations of differing ownership, and substations within line-of-sight to each other.

Finally, while NERC is not recommending an expansion of the CIP-014 Applicability criteria at this time, NERC finds that, given the increase in physical security attacks on BPS substations, there is a need to evaluate additional reliability, resiliency, and security measures designed to mitigate the risks associated with those physical security attacks. As discussed further below, establishing a uniform, bright line set of minimum physical security protections for all (or even an additional subset of) BPS substations and associated primary controls centers, is unlikely to be an effective approach to mitigating physical security risks and their potential impacts on the reliable operation of the BPS. While a uniform set of minimum level of protections could potentially prevent some forms of physical security threats, NERC finds that such a pursuit lacks the application of a risk-based approach to expending industry resources, fails to provide for a methodical approach necessary to address site-specific threats or objectives (as expected using a design basis threat process), and does not consider the need for other reliability, resiliency, and security measures to mitigate the impact of a physical attack. These combined measures provide increased operational and planning capability as well as improved effectiveness of local network restoration. NERC finds that this more holistic approach will provide greater long-term flexibility and minimize the impacts of physical attacks on BPS reliability.

To that end, NERC recommends further evaluation of the appropriate combination of reliability, resiliency, and security measures that would be effective in helping to mitigate the impact of physical security attacks. Following issuance of this report, NERC will work with FERC staff to hold a technical conference to gather additional data on these matters and discuss whether and how those measures should be incorporated into NERC’s mandatory Reliability Standards. NERC will consult with FERC in the development of the technical conference to discuss, among other things, the following topics:

- The appropriate risk-based approach to identifying the objective of any minimum level of protections, risks to be mitigated, and industry resources necessary to meet such minimum requirements.
- Expanding the use of planning studies, conducted by Transmission Planners (“TPs”) under Reliability Standard TPL-001 to evaluate physical security attacks, identify applicable study criteria, and contain a corrective action plan to mitigate inadequate performance against such criteria.

-
- Enhancing Operational Planning Assessments to include loss of assets (transmission or generation) from physical attacks.
 - Enhancing TP and TO requirements to ensure spare equipment pool strategies are adaptive, in-sync, and provide sufficient wide area coverage.
 - Requiring Reliability Coordinators (“RCs”) to develop and train to readiness scenarios reflecting a physical security incident with TOs, TOPs, Generator Owners, and Generator Operators.

NERC will use the information learned during the technical conference described above to determine the next steps, including potential Reliability Standards modifications.

NERC will also continue its significant efforts outside the context of mandatory Reliability Standards to mitigate the potential for and impact of physical security attacks across the grid. NERC, through the E-ISAC and other mechanisms, has worked extensively with industry to raise awareness of physical security threats and vulnerabilities and develop tools and guidance to promote and facilitate enhanced physical security protection and response measures across the industry. The E-ISAC established the Physical Security Advisory Group, which is an E-ISAC-led group comprised of industry participants that provides expertise to advise industry on threat mitigation strategies to enhance the BPS’s physical security and reliability. The E-ISAC regularly holds Vulnerability of Integrated Security Analysis (“VISA”) workshops at utility facilities to demonstrate how to implement the VISA process. The VISA process is a scenario-based, vulnerability assessment tool to analyze the effectiveness of security measures to prevent, detect, delay, and respond to attacks. The E-ISAC has also recently released materials to aid and assist entities to better prepare their assets against malicious physical attacks. These materials include the *Physical Security Resource Guide for Electricity Asset Owners and Operators*, which is available on the E-ISAC portal.⁴

⁴ Available at: <https://eisac-portal.force.com/eisacportal/s/article/E-ISAC-Physical-Security-Resource-Guide-January-2023>.

Background

CIP-014 Development and History

NERC initially developed the CIP-014 Reliability Standard in response to a Commission order issued March 7, 2014 in Docket No. RD14-6-000 directing NERC to submit for approval one or more Reliability Standards to address physical security risks and vulnerabilities to critical BPS substations and control centers.⁵ In the March 2014 Order, the Commission determined that physical attacks on the BPS could adversely impact reliable operation of the BPS, resulting in instability, uncontrolled separation, or Cascading failures. The Commission noted that the then current Reliability Standards did not specifically require registered entities to take steps to protect against physical security attacks on the BPS. Accordingly, the Commission directed NERC to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of BPS “critical facilities.”

The March 2014 Order indicated that the Reliability Standards should require owners or operators of the BPS to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the BPS: (1) owners or operators of the BPS should perform a risk assessment of their systems to identify their “critical facilities”; (2) owners or operators of the identified “critical facilities” should evaluate the potential threats and vulnerabilities to those identified “critical facilities”; and (3) those owners or operators of “critical facilities” should develop and implement a security plan designed to protect against attacks to those identified “critical facilities” based on the assessment of the potential threats and vulnerabilities to their physical security. In the March 2014 Order, the Commission stated that a “critical facility” is “one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.”⁶

On May 23, 2014, NERC petitioned the Commission to approve Reliability Standard CIP-014-1. NERC explained that Reliability Standard CIP-014-1 “serves the vital reliability goal of enhancing physical security measures for the most critical [BPS] facilities and lessening the overall vulnerability of the [BPS] to physical attacks.”⁷ NERC stated that the “appropriate focus of the proposed Reliability Standard is Transmission stations and Transmission substations, which are uniquely essential elements of the [BPS].”⁸ As noted above, consistent with the March 2014 Order, the purpose of the CIP-014 Reliability Standard is “identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an interconnection.” The Commission approved CIP-014-1 on November 20, 2014 in Order No. 802, finding that the standard satisfied the directives in the March 2014 Order.⁹

The CIP-014 Applicability criteria match the “Medium Impact” criteria for transmission facilities listed in Attachment 1 of Reliability Standard CIP-002-5.1a. The Facilities include:

1. Transmission facilities operated at 500 kV or higher;
2. Transmission facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and that exceeds an “aggregated weighted value” as defined in the standard;

⁵ Reliability Standards for Physical Security Measures, 146 FERC ¶ 61,166 (2014) [hereinafter March 2014 Order].

⁶ *Id.* at P 6.

⁷ NERC, *Petition of NERC for Approval of Proposed Reliability Standard CIP-014-1*, Docket No. RD14-6-000 at 15-16 (Mar. 7, 2014).

⁸ *Id.* at 18.

⁹ *Physical Security Reliability Standard*, Order No. 802, 149 FERC ¶ 61,140 (2014). Since the issuance of Order No. 802 the Commission approved minor modifications to the CIP-014 standard to remove the term “widespread” to Requirement R1 and to remove the provision from the Compliance section that required all evidence demonstrating compliance with the standard to be retained at the Transmission Owner’s or Transmission Operator’s facility.

-
3. Transmission facilities at a single station or substation location that are identified by its Reliability Coordinator (“RC”), Planning Coordinator (“PC”), or Transmission Planner (“TP”) as critical to the derivation of Interconnection Reliability Operating Limits and their associated contingencies; and
 4. Transmission Facilities identified as essential to meeting nuclear plant interface requirements.

The CIP-014-1 Standard Drafting Team adopted these Applicability criteria as the Commission had previously approved them as a technically sound basis for identifying Transmission Facilities, which, if compromised, would present an elevated risk to the BPS.

FERC Order Directing Study of CIP-014

On December 15, 2022, the Commission directed NERC

to conduct a study evaluating (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard CIP-014-3 (Physical Security Reliability Standard); (2) the required risk assessment set forth in the Physical Security Reliability Standard; and (3) whether a minimum level of physical security protections should be required for all Bulk-Power System transmission stations and substations and primary control centers.¹⁰

The Commission directed that NERC submit a report to the Commission on the study’s findings and recommendations within 120 days of the date of the order.¹¹

The Commission explained that it was directing this evaluation because “there has been an increase in reports of physical attacks on electric substations” in recent months, some of which resulted in customer outages.¹² In particular, the Commission cited the December 3, 2022 physical attacks on substations in Moore County, North Carolina, the November 2022 incidents at several Pacific Northwest substations, and that Federal authorities disrupted recent planned attacks before they were perpetrated.

¹⁰ December 2022 Order at P 1.

¹¹ *Id.*

¹² *Id.* at P 6.

Data Inputs

This section describes the scope of the data reviewed, sources of CIP-014 subject matter expertise, and more general physical security experts consulted to conduct this evaluation and substantiate the report findings. As discussed below, to conduct this evaluation, NERC gathered data from various ERO Enterprise groups and planning cases. Further, NERC identified substation kV class and adjacency using the transmission models representing the Facilities of the Bulk Electric System, and used that data as part of this evaluation.

Regional Entity Subject Matter Experts

Regional Entity subject matter experts (“SMEs”) provided their perspectives, data, and insights throughout the assessment. These SMEs reviewed the content of this report for clarity, the completeness of the conclusions, and the engineering judgement used to support the recommendations. NERC will continue to engage Regional Entity SMEs for ongoing physical security threat activities.

Electric Information Sharing and Analysis Center

Finally, NERC consulted the Electric Information Sharing and Analysis Center (“E-ISAC”) for data on recent physical security attacks, the nature of physical security threats and vulnerabilities, and best practices for implementing physical security protections. In particular, this consultation leveraged E-ISAC BPS physical security threat experience and awareness to support the findings within the section of this report pertaining to an evaluation of “minimum level of physical security” at all BPS substations and associated primary control centers.

Review of Planning Case Data

This report uses the topology of Interconnection-wide base cases to estimate the number of BPS substations in the Interconnection. Those estimates are based on the following criteria:

- The high side and low side of a transformer are located in the same substation;
- If it exists, the terminals of a circuit breaker are located in the same substation;
- The terminals of series capacitors are in the same substation;
- The terminals of multi-section lines are in different substations (e.g., tapping of a line); and
- A substation has a significant impedance between its neighboring substations.

The topology estimates assumed that a substation impedance¹³ would have a greater than 0.2km distance. A high-end estimate (signifying a lower count of estimated substations) increases this distance to 1 km. Using these criteria, the maximum amount of substations found in each interconnection are found in **Table 1**. Also included are estimations from Form EIA-860 data in a separate row and the estimations of the topology including only Bulk Electric System substations found.¹⁴ Differences in the EIA data forms and the planning model representing a substation account for the numerical differences between the models. The primary difference is that the planning model estimates may count multiple generator unit buses (if modeled explicitly) feeding the primary substation and switchyard to the plant. With the EIA data this is counted as one substation, while the planning model may count this as multiple due to isolating on impedance. The topology estimate of the planning model, however, can readily provide connected substations, ratings of the lines connecting the substations, and the lines’ nominal kV.

¹³ Impedances in the Interconnection-wide base cases are typically in per unit (p.u.), meaning they are a function of the system base MVA and their nominal kV. This check for distance converts the p.u. of the line into a regular impedance (in Ohms) and uses an assumed impedance per mile when comparing to this distance threshold.

¹⁴ The U.S. Energy Information Administration’s Form EIA-860 collects generator-level specific information about existing and planned generators and associated environmental equipment at electric power plants with 1 megawatt or greater of combined nameplate capacity.

Data Inputs

Table 1: Estimation of Substations

Source	EI	TI	WI
Topology Estimate	56,767	5,236	11,948
Topology Estimate (only BES)	25,000+	3,662	7,854
Energy Information Agency (U.S. Only)	40,608	2,546	10,992
Energy Information Agency (BES U.S. Only)	39,000	3,500	10,000

The information in **Table 1** can be graphically compared to **Figure 1** which uses the planning case estimates and **Figure 2** which uses the EIA data sources. Comparing the ratios currently applicable to CIP-014-3 (>345 kV, >200 kV, >100 kV) and all other buses in the data source indicates that both data sets contain roughly the same percentage of substations. Again, this indicates that the topology estimation using the planning case data is a representative sample of all substations in each Interconnection, and that the percentage composition of these substations is generally aligned. Based on these comparisons and the benefit of other data fields of the planning model, the team favors analysis using the planning model numbers for assessing the adequacy of CIP-014-3’s Applicability criteria.

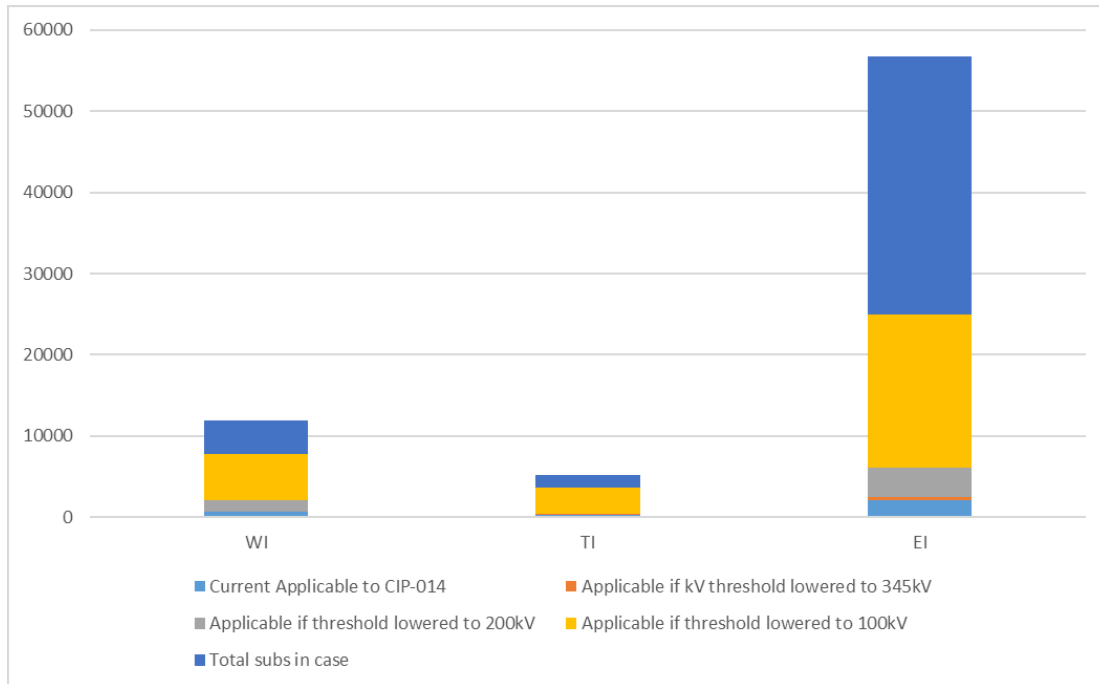


Figure 1: Substation Topology Estimates Using Planning Cases

Data Inputs

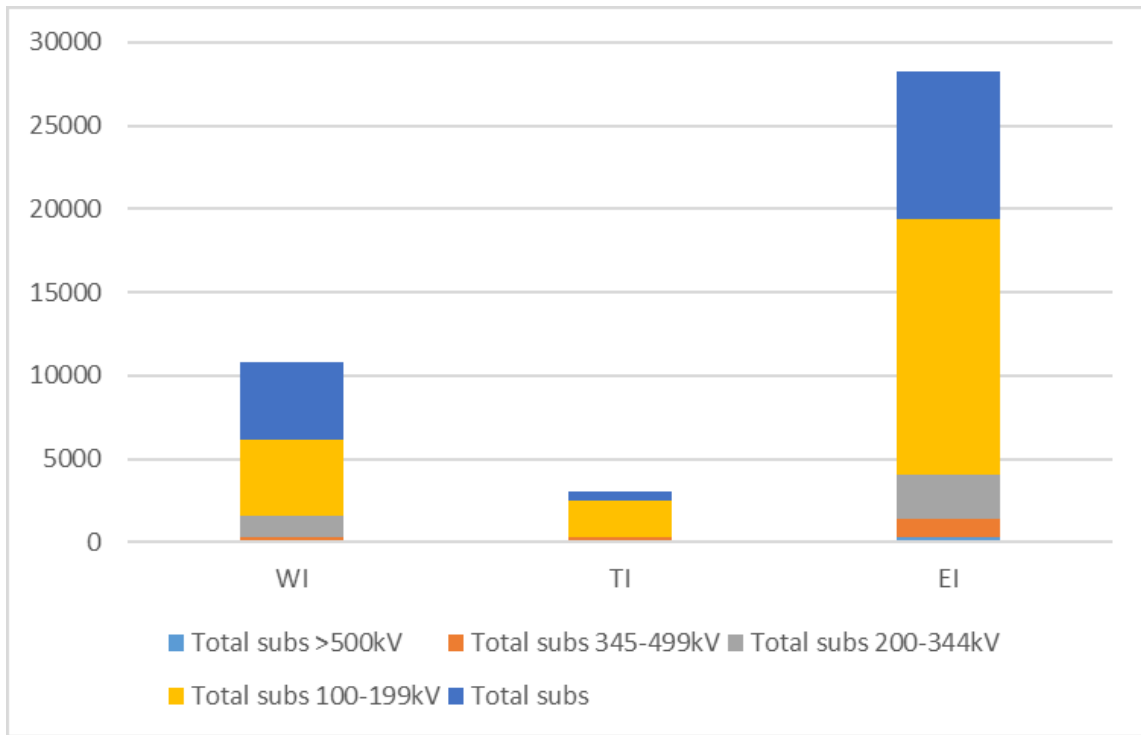


Figure 2: Substation Classification Using EIA data

Evaluation of CIP-014 Applicability Criteria

Reliability Standard CIP-014 is designed to identify those “critical” facilities that would present significant risks to the reliability of the BPS if damaged or rendered inoperable as a result of a physical attack. The expectation in the Commission’s March 2014 Order directing the development of the standard was that a limited number of substations would be identified in the risk assessment as having the type of adverse impact on the Interconnection the standard was designed to mitigate. Consistent with that expectation and to help ensure that industry resources were properly focused on those Facilities that present an elevated risk, CIP-014 uses a screening approach to determine which facilities should be assessed.

NERC finds that the objective and screening approach of CIP-014 continues to appropriately focus limited industry resources on risk to the reliable operation of the BPS associated with physical security incidents at the most “critical” facilities. Based on studies using available data, NERC finds that the CIP-014 Applicability criteria is meeting that objective and is broad enough to capture the subset of applicable facilities that TOs should identify as “critical” pursuant to the Requirement R1 risks assessment. As explained below, NERC did not find evidence that an expansion of the Applicability criteria would identify additional substations that would qualify as “critical” substations under the CIP-014 Requirement R1 risk assessment. Accordingly, at this time, NERC is not recommending expansion of the CIP-014 Applicability criteria. NERC acknowledges, however, that supplemental data¹⁵ could show that additional substations configurations would warrant assessment under CIP-014 and plans to continue such evaluation, as described below.

Analysis of Applicability Criteria

The CIP-014 Applicability criteria represent different indicators of higher potential risk to identify a subset of substations, referred to herein as the applicability list, that should be subject to the Requirement R1 risk assessment. The Applicability criteria of CIP-014 consists of four criteria, further analyzed in the sections below. These four criteria are:

- A Voltage inclusion criterion (applicability criterion 4.1.1.1);
- A weighting factor inclusions criterion (applicability criterion 4.1.1.2);
- An inclusion for Transmission Facilities that are identified by a RC, PC, or TP as critical to the derivation of an Interconnection Reliability Operating Limit (“IROL”) and their associated contingencies (applicability criterion 4.1.1.3); and
- An inclusion for Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements (applicability criterion 4.1.1.4).

Voltage Inclusion Criterion

The voltage inclusion criterion brings in all transmission facilities operating at 500 kV or higher. The inclusion of all substations with 500 kV transmission facilities is an appropriate bright-line criterion for identifying a potentially critical substation.

Weighting Factor Inclusion Criterion

The criterion aligns with CIP-002-5.1a Impact Ratings for medium impact BES Cyber System (BCS), criterion 2.5. This criterion uses a combination of aggregated transmission line weighting values, as shown in [Table 2](#), along with a minimum number of distinct substation connections. This criterion includes transmission facilities that are operating between 200kV and 499kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other substations and has an “aggregate weighted value” exceeding 3000.

¹⁵ Namely, expansion plans, future year realized conditions, impacts of grid transformation, and other similar projections that alter year-to-year. These, in aggregate, could alter substation configuration.

Evaluation of CIP-014 Applicability Criteria

Table 2: CIP-014-3 Line Weighting Criteria

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

NERC notes that CMEP evaluations of registered entity practices for substation applicability list development provided additional insight on different approaches for determining line counts. Unique variations of certain substations add complexity to the aggregated weighting, such as split buses, ring buses, multiple ownership configurations, and other topology variations that may need a human evaluation to ensure that registered entities correctly count lines and connecting substations. Currently, there is insufficient data regarding the extent of observed approaches that do not align with ERO Enterprise expectations and whether modifying the Reliability Standard to add clarity regarding line count methods is warranted. CMEP staff will continue to leverage the CMEP Practice Guide for CIP-014-3 R1¹⁶ when performing compliance and risk determinations and assure CMEP program alignment.

Substations with Partial Criterion Applicability

To determine whether the weighting factor criterion is adequate to meet the objective of CIP-014, NERC looked to identify what types of substations would not fully meet this criterion but did include some partial characteristics. Initially, NERC identified a limited number of topology configurations for substations with line weightings that were close to but below the aggregated value of 3000. These topology configurations include substations with:

- 230 kV (4 or less lines) totaling 2800;
- 345 kV (1 or 2 lines) totaling 1300 and 2600 respectively; and
- 345 kV (1 line) and 230 kV (1 or 2 lines) totaling 2000 and 2700 respectively.

NERC also identified substations that could exceed an aggregated line weighting of 3000 but would not be required to be included within the risk assessment because they: 1) only connected to one or two other substations and 2) the other applicability criteria did not apply.

Based on the data available at the time of this report, NERC sought to analyze the potential impact of the loss of existing substations with these two types of partially applicable criterion (i.e., those close to but below the 3000 weighting and those over 3000 but with only one or two other connections). As explained below, using data available from CMEP activities and planning cases, NERC did not identify any instances where an entity had substations meeting these characteristics (and thus excluded from the CIP-014 risk assessment) that would have had the adverse system impacts that CIP-014 is designed to identify. While expanding the CIP-014 applicability criteria to include these types of substations would provide for a larger pool of substations to assess under Requirement R1, there is no indication that an expansion of the weighting factor inclusion criterion is warranted for the purpose of identifying additional “critical” substations.

The following is an explanation of NERC’s approach to evaluating the adequacy of the weighting factor criterion. Specifically, NERC performed a preliminary screen of steady-state data as well as a sensitivity analysis. The details and results of these evaluations are included below.

¹⁶ NERC, *ERO Enterprise CMEP Practice Guide: CIP-014-3 R1* (Sept. 2022), <https://www.nerc.com/pa/comp/guidance/CMEPPPracticeGuidesDL/CMEP%20Practice%20Guide%20CIP-014-3%20R1.pdf>.

Evaluation of CIP-014 Applicability Criteria

Steady-State Preliminary Screen

As a preliminary screening test, NERC analyzed the outage of each substation in steady-state Contingency processing tools in both a heavily and lightly loaded condition. This screen provided an indication of whether substations that fall outside of the aggregate 3000 line-weighting criteria could potentially cause the adverse impacts that CIP-014 is designed to prevent. **Table 3** demonstrates the findings of this screen. The difference between the total number of substations versus the total number of solved and unsolved Contingencies is explained by the fact that the Contingency processor did not reflect in service substations only. Thus, a number of substations identified for Contingency were skipped due to being modeled in the chosen cases as out-of-service. NERC staff counted the unique set of Contingencies between the cases, reflected in **Table 3**. NERC staff spot tested the number of not solved Contingencies and the majority were determined to be a numerical or model issue that is resolved by correcting the elements. Further, spot testing the Contingency with a transient dynamic simulation for the most overloads or voltage violations demonstrated that the system stayed stable during these extremes. The results of this steady-state preliminary screen do not indicate that modification to the applicability criteria is needed at this time. This further supports the conclusion that the substations in question are relatively smaller than those substations covered by the current CIP-014 applicability and, as such, are less likely to cause instability, uncontrolled separation, or Cascading if rendered inoperable.

Table 3: Steady-State Preliminary Screen Results

Assessment Metric	Count
Total Number of Substation Contingencies	22,514
Total Unique Substation Contingencies	11,784
Total Number Solved	17,070
Total Number Not Solved	445
Maximum Count of Overloads in a Single Contingency	8
Maximum Count of Voltage Violations in a Single Contingency	261
Number exhibiting instability, Uncontrolled Separation, or Cascading	0

A more thorough technical analysis, such as the inclusion of a dynamic study, would need to be performed in each instance to further confirm the conclusion as potential impacts will vary depending on the electrical characteristics of the connected network. Studies for substations above 3000 but with only one or two connections may already be covered by an assessment required by Reliability Standard TPL-001 as the Contingencies selected for TPL-001 include single line outages and common tower outages that include two or more lines out of service. However, TPL-001-5.1 currently does not require the evaluation of the loss of all elements within a substation to evaluate the other identified instances of partial criterion applicability. NERC will continue to assess the effectiveness of CIP-014's Applicability Criteria to determine if any of these configurations would result in a critical identified substation.

Sensitivity Analysis for Potential Scope Increase

To further NERC's understanding of the potential scope of substations subject to the CIP-014 Applicability criteria, NERC conducted an analysis to estimate the total populations of included versus excluded substations. NERC receives electric models of the Interconnection (e.g., steady-state and dynamic transient models) through the Reliability Standard MOD-032 process. NERC applied different approximated criteria alterations to these Interconnection cases to evaluate impacts and estimate the number of substations that could be applicable under different criteria.

Adjusting just the voltage applicability criteria (4.1.1.2), **Figure 3** displays the percentage of substations in the planning models that would currently be applicable to CIP-014 using the topology estimation tool and the upper bound of substations. **Table 3** separates the Western Interconnection (WI), Texas Interconnection (TI), and Eastern Interconnection (EI) into different bars in **Figure 1** for each voltage levels. These are to mirror the lower kV of the

Evaluation of CIP-014 Applicability Criteria

CIP-014 line weighting criterion to determine the upper bound of applicability changes to the number of substations currently assessed per the Requirement R1 risk assessment. This demonstrates the enhanced study rigor and scope of the standard should the applicability criteria be altered to include more substations, but does not speak to if those added substations would be deemed “critical.” The >100 kV section shows substations that would meet the normal BES definition cutoff.

As demonstrated in the graph, the number of substations currently applicable (per 4.1.1.1 and 4.1.1.2) is around 10 percent. Lowering the voltage applicability from 500kV threshold to 345kV keeps the percentage of applicable substations to approximately 10 percent. This is due to the fact that current CIP-014 applicability covers the large majority (>85%) of 345kV substations. To expand the substations applicability in a significant manner, the voltage threshold would need to include substations >200 kV to increase the percentage coverage of substations in a significant way (by five percent or more). Modifying the voltage applicability to include all BES represented buses would ensure 100% of all substations be applicable to the risk assessment.

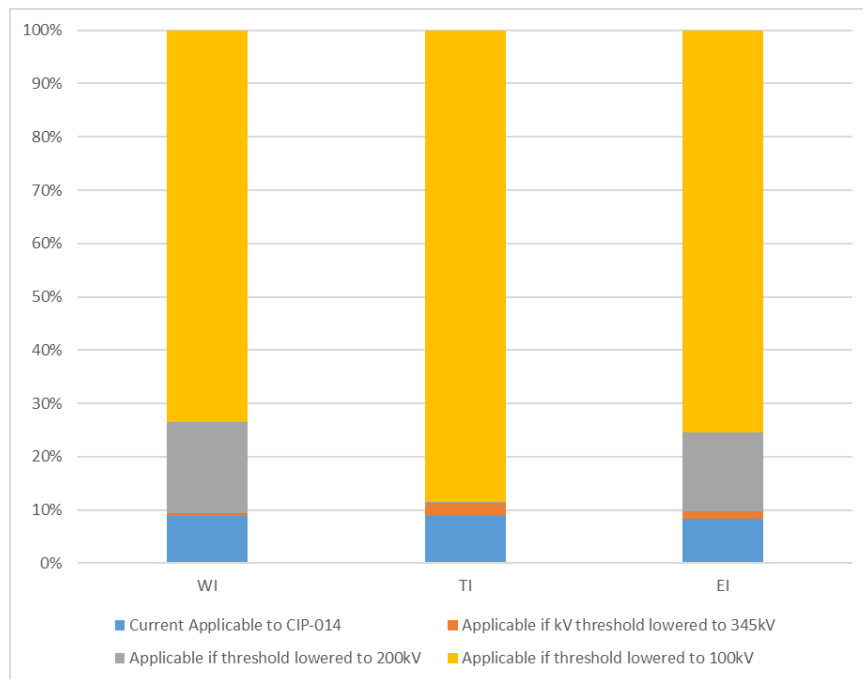


Figure 3: Estimated Percentage of Substations Applicable

The results of this sensitivity analysis do not provide any indication that modification to the applicability criteria is needed to capture additional “critical” substations. Similar to the results of the preliminary screen, determining that the applicability list includes a large enough set of the total population is challenging without conducting a full risk assessment for all stations. The justification for the CIP-014 risk-based screening approach – i.e., to study only those stations that meet a high bar of criteria – remains appropriate. As only very few of the currently studied substations are identified as critical, the screening approach continues to be reasonable. Engineering judgment will also show that the lower kV substations typically do not influence the remainder of the BPS as great as the larger, higher kV class substations. As **Figure 3** demonstrates, the kV class criterion can be altered to increase the amount of substations included in the risk assessment, but only lowering to >200kV would provide a substantial increase in the amount of substations for the study. Further, the applicability increase doesn’t necessitate any of those added substations being deemed “critical” per the risk assessment as indicated previously in **Table 3**.

Based on the results of the preliminary screen and sensitivity analysis, NERC has not identified any new information that would warrant expanding or modifying the weighting factor criterion at this time. NERC plans, however, to continue evaluating the adequacy of this Applicability criterion in meeting the objective of CIP-014. NERC recognizes

Evaluation of CIP-014 Applicability Criteria

that supplementary data could show that additional substations configurations would warrant assessment under CIP-014. The supplementary data would include expansion plans, future year realized conditions, impacts of grid transformation, and other similar projections that alter year-to-year. These, in aggregate, could alter substation configuration. Accordingly, NERC recommends holding a technical conference to, among other things, identify the type of substations it should study and establish data needs for conducting studies on those substations to determine whether they should be included in the weighting factor criterion. NERC plans to consult with FERC staff on the content, timing, and logistics for holding the technical conference.

Inclusion Criterion for Transmission Facilities Identified by Other Registered Entities

This criterion in CIP-014's Applicability provides additional assurance that registered entities with other functional obligations to study adverse impacts to the Interconnection have direct input to the applicability list for CIP-014-3. There is a standard development project in progress addressing potential changes to language in CIP-002 and CIP-014 to clarify these roles and tasks. NERC Reliability Standard Project 2021-03¹⁷ addresses the responsibility of RC, PC, and TPs in identifying Facilities that warrant CIP-014-3 consideration; specifically to address TPs and PC functions language relating to inclusion of Facilities critical to the derivations of IROLs.

As stated in the NERC 2022 CMEP Implementation Plan,¹⁸ NERC and the Regional Entities conducted a joint review with RCs to understand how RCs are performing their analysis and determining IROLs, including how the RCs incorporate the recommended practices outlined in NERC *Reliability Guideline – Methods for Establishing IROLs*.¹⁹ The results of this IROL joint review are not publicly available at the time of this report. NERC intends on sharing the results with the Project 2021-03 Standard Drafting Team to consider during the standards modification process.

Note that if a TO completes CIP-014-3 R1 risk assessment and found no stations that meet the criteria specified in Applicability Section 4.1.1, the TO doesn't have a requirement to conduct another risk assessment for the next 60 calendar months. If the RC/PC/TP declares the station as critical to the derivation of an IROL and its associated contingencies after the TO has completed its risk assessment, the TO still does not have to do another assessment until its 60 calendar months mark. This offset on the periodicity of the R1 risk assessment based on CIP-014 Applicability changes is discussed more in the evaluation of the R1 risk assessment where NERC recommends an alignment of this periodicity. This issue, however, is not an indication of altering the scope of applicable Facilities but on how often they are studied in Requirement R1.

Inclusion Criterion for Transmission Facilities Meeting Nuclear Plant Interface Requirements

The inclusion criterion for those Transmission Facilities meeting Nuclear Plant Interface Requirements is an appropriate threshold for a identifying a potentially critical station.

Impact Assessment of Recent Attacks on Applicability

Recently reported physical attacks resulted in the loss of end-use customers and the ability to serve load through a portion of the high voltage network. These attacks, however, did not result in instability, uncontrolled separation, or Cascading. Specifically, NERC determined that substations attacked in Moore County, North Carolina that the December 15 Order references would not have been covered by the CIP-014-3 applicability. The referenced attack left multiple geographically close substations damaged, resulting in the loss of end-use customer load. Based on the topology, the substations attacked do not meet the line weighting for the applicability list. The attack rendered one BES substation inoperable and did not result in instability, uncontrolled separation, or Cascading for the Interconnection. These facts about the attack indicate that even if the substation were subject to Requirement R1

¹⁷ The Project 2021-03 – CIP-002 Communications Protocol Converters webpage is available at <https://www.nerc.com/pa/Stand/Pages/Project%202021-03%20CIP-002%20Transmission%20Owner%20Control%20Centers.aspx>.

¹⁸ NERC, *2022 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan* (Oct. 2021), <https://www.nerc.com/pa/comp/CAOneStopShop/ERO%20CMEP%20Implementation%20Plan%20v1.0%20-%202022.pdf>.

¹⁹ NERC, *Reliability Guideline – Methods for Establishing IROLs* (Sept. 2018), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf.

Evaluation of CIP-014 Applicability Criteria

risk assessment, the loss of the BES substation in the attack would not result in instability, uncontrolled separation, or Cascading. Placing CIP-014 type physical protections on those stations that do **not** cause instability, uncontrolled separation, or Cascading is not consistent with CIP-014's purpose of identifying and protecting the substations that would cause instability, uncontrolled separation, or Cascading. Physical protections against these types of attacks is covered later in this report discussing minimum physical security protections for all BPS substations.

Adequacy of Applicability Criteria Conclusions

In sum, based on available data, the Applicability criteria in Reliability Standard CIP-014-3 appears to adequately identify the subset of all transmission stations and substations that TOs should evaluate as part of the Requirement R1 risk assessments. A large majority of those stations currently studied in the risk assessments will not be identified as critical and there are no current studies that indicate an expansion of the Applicability criteria will identify additional stations that would qualify as "critical substations" under the Requirement R1 risk assessment.

NERC will continue to assess and conduct oversight of CIP-014-3 implementation around applicability list development and maintenance. NERC will also conduct engineering assessments to ensure the applicability is effectively covering the various configurations of transmission substations. Along with the recommendations to hold a Technical Conference for minimum level of security, NERC will, among other things, establish additional study and data needs to confirm its analysis as demonstrated in this report. More details on the recommended Technical Conference are found in the section [Evaluation of Minimum Level of Physical Security Protections](#).

Evaluation of Requirement R1 Risk Assessment Adequacy

Analysis

The CIP-014 Requirement R1 risk assessment requires applicable TOs to study whether the loss of an applicable substation could result in instability, uncontrolled separation, or Cascading. While the objective of these assessments is appropriate, NERC finds that there should be additional clarification as how registered entities must conduct the assessments. In reviewing its CMEP data, NERC found that registered entities have inconsistent approaches to performing the risk assessment and they did not always meet the technical rigor expected for other planning horizon study assessment-related Reliability Standards, such as TPL-001. This report aggregates the issues identified to date for risk assessment adequacy by 1) deficiencies introduced into the models²⁰ used within the risk assessment, and 2) insufficient technical studies, including insufficiently documented technical rationale.

Risk Assessment Deficiencies Caused by an Entity's Model Decisions

While the Requirement R1 risk assessment is applicable to TOs, not all TOs have in-house SMEs to conduct the studies. TOs are largely aware of their own assets and can identify nameplate information, cybersecurity impacts, and applicability inside the boundaries of their substations. However, while the TO may be an expert in identifying their equipment and its location, TOs often lack in-house expertise to study Interconnection-wide electrical impact, which requires specific tools, data, and analysis of simulation outcome. Collectively, these issues complicate a TO's thorough understanding and review of modeling decisions and justifications made by other entities responsible for model curation such as TPs and PCs. Further, CMEP personnel have identified that these modeling decisions do not apply consistent engineering practices and often either introduce inappropriate future projects or apply inappropriate study periodicity.

Inappropriate Future Projects

Based on ERO stakeholder engagement and CMEP observations, many TOs have been seeking clarity regarding how the risk assessment window for the initial and subsequent assessments overlapped with projects considered in-scope for the risk assessment. As a registered entity leverages Interconnection-wide base cases to perform the CIP-014-3 Requirement R1 risk assessment, the base case availability plays a part in a registered entity's responsibilities.

Applicable registered entities are required to perform the CIP-014-3 Requirement R1 risk assessment at least once every 60-calendar months or 30-calendar months, depending on whether or not the previous risk assessment identified any critical substations. Risk assessments are required to include existing substations and those planned to be in-service within 24 months of the risk assessment. This indicates that there are two paths taken based on the outcome of the R1 risk assessment. The two paths are as follows:

1. If the assessment for in-service equipment 24 months in the future designates at least one critical substation, conduct the next risk assessment within 30 months, and
2. If the assessment for in service equipment 24 months in the future designates no critical substations, conduct the next risk assessment after 60 months.

A registered entity has the flexibility to conduct this 24-month look ahead risk assessment on a more frequent basis. However, the Interconnection-wide base cases typically are built on an annual frequency causing additional complexity. It is unlikely that more frequent risk assessments will produce differing results due to the base case creation timelines. [Figure 4](#) graphically illustrates the timeline between the end of the risk assessment and the next time a registered entity is required to perform a subsequent risk assessment.

²⁰ "Models" herein refer to the aggregated set of electrical components and characteristics used by power flow software programs to: 1) evaluate and monitor Real-time conditions, 2) evaluate the efficacy of planned system changes for Transmission, generation, and forecasted changes to demand/load, and 3) simulate Contingencies such as events, severe weather, faults, etc. to test the resiliency of the area studied.

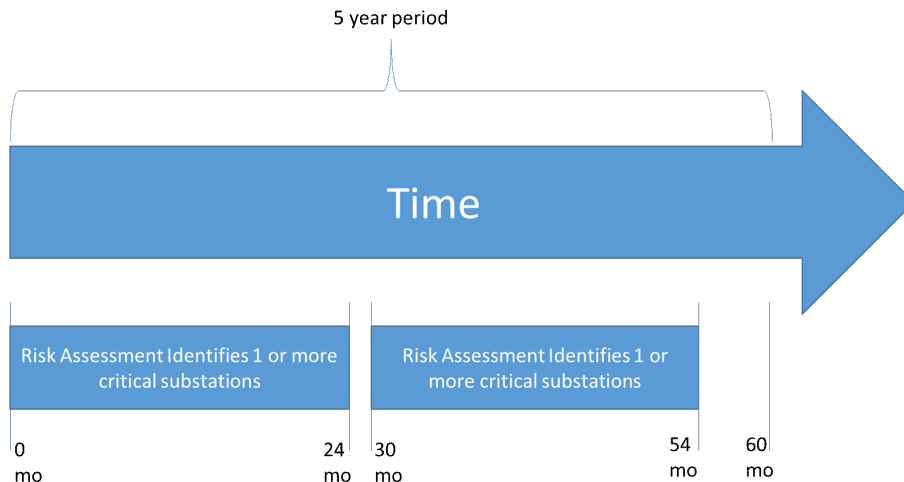


Figure 4: Current CIP-014 R1 Risk Assessment – Using 30 Months

CIP-014-3 requires that a registered entity must include projects that will be in-service within the next 24 months but does not provide a full-time range of acceptable projects to include. For example, in the case of the 30-month frequency of study, TOs are often provided a 5-year model by their TP or RC.²¹ The result of the registered entities having the 5-year model allows it to include projects that the TP or RC have projected be in-service for dates beyond the next two risk assessments. CMEP staff often observe the inclusion of these projects during CMEP activities and through NERC Oversight.

There is a different concern when there are no critical substations identified during the previous risk assessment, as shown in Figure 5. As a result, this introduces a potential that the risk assessment fails to include all in-service projects through the full time period between risk assessments. In both cases, the ability to effectively and consistently identify critical stations within the 5-year horizon may be negatively impacted.

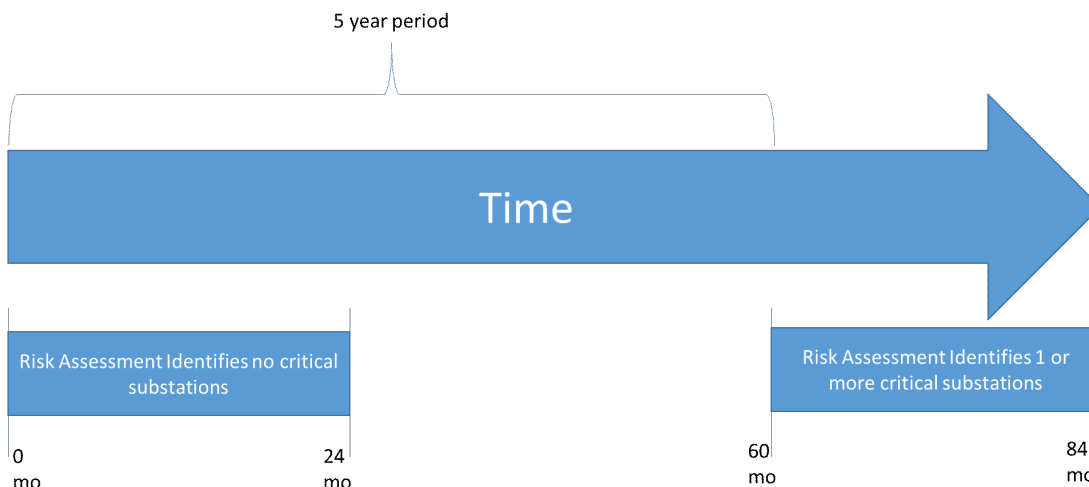


Figure 5: Current CIP-014-3 R1 Risk Assessment – Using 60 Months

²¹ Within transmission planning studies, a 5 year (or 60 month) period is generally used to scope the Near-Term Planning Horizon.

Evaluation of Requirement R1 Risk Assessment Adequacy

A TO may conduct more frequent risk assessments, but the obligation allows for a 30-month periodicity when a TO identifies a critical substation. Per the technical rationale for CIP-014:²²

The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates.

Each TO is required to submit their expected in-service projects for the Interconnection-wide models used to assess the stability of the Interconnection. It is during that stage that surrounding TO projects are included.

Further, this technical rationale refers to the planning cycle and frequency that a TO constructs substations. This is dissimilar from how TPs build models to conduct long-term planning assessments. This introduces discrepancies in decisions made regarding the use of models and what the registered entity considers appropriate to include within the study and the number of years studied.²³

Inappropriate Study Periodicity

CIP-014-3 periodicity is different between registered entities that do not have critical identified substations and those that have previously identified critical substations. The CIP-014-3 Requirement R1 risk assessment must evaluate impacts to the Interconnection that necessitate the need for models used during each registered entity's risk assessment to include up to date models of neighboring systems. While a registered entity may not have identified critical stations in their footprint, the modification of the system in future years may result in changes to system flows that could influence risk assessment results. As the periodicity between neighboring registered entities may be different (up to 30-60 months), there may be a gap in risk assessment efficacy during years project update data does not overlap with study periods.

A risk assessment conducted without this update to surrounding facilities can influence the quality of the assessment as facilities not in-service pose challenges with conducting the risk assessment and the quality of the assessment's results. While the technical rationale for this flexibility is appropriate for a single TO, it does not effectively apply to all areas where surrounding transmission buildouts may influence the remainder of the interconnected system. For this reason, registered entities should understand and mitigate the allowable 6 month to 36-month²⁴ reassessment delay.

Registered entities must mitigate the issues presented by risk assessment modeling decisions to require when a critical substation is identified within a planning footprint to assess the impact of the project. One method to accomplish this is to require areas that have identified critical substations to consistently assess the impact of their and neighboring facilities have on the loss of the identified critical substation. One example of how registered entities can consistently assess the impact of critical substations is by lowering the 30-month window to 24 months as shown in **Figure 6**. This method would alter the quantity of assessments performed by registered entities; however, the alteration is minor.²⁵ This is not the only way to make the timelines consistent with project submittals and updates to transmission in a registered entity's footprint. Registered entities should explore alternative options to ensure alignment of the risk assessment cycle and a systematic project update for surrounding TOs.

²² CIP-014-3 is available here: <https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf>.

²³ Transmission Planners are required to annual study forecasted system changes for Year 1 (or Year 2) and Year 5 at a minimum. Planners will often study additional future years depending on their own practices and system needs.

²⁴ Should a neighboring set of two entities not have critical facilities, the period gap between the end of the risk assessment period (24 months) and the subsequent risk assessment (at 60 months) is 36 months total of potential transmission assets not assessed for their potential impact or identification of critical substations.

²⁵ Mathematically, over a 10 year period this increase is one extra study.

Evaluation of Requirement R1 Risk Assessment Adequacy

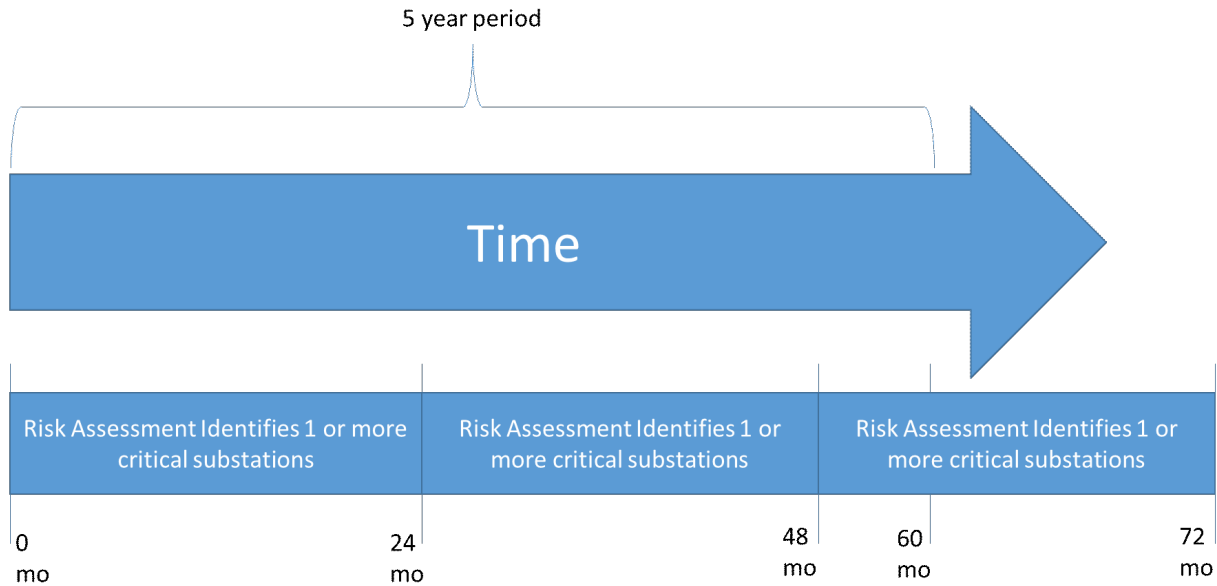


Figure 6: Example of Resolved Risk Assessment Periodicity

Insufficient Technical Studies Including Insufficiently Documented Technical Rationale

To accomplish the risk assessment, TOs are required to use models to simulate and evaluate the loss their equipment poses to the Interconnection. TO’s substantiate these risks by evaluating electrical responses for violations of different criteria used in the study of instability, uncontrolled separation, or Cascading. Determinations of effective and sufficient criteria necessitate technical expertise. The accuracy and validity of model data, operational studies, and long-term studies are often the subject of NERC reliability guidelines, alerts, and CMEP activities. TOs that are not also regularly involved in TP studies and current reliability concerns are unlikely to provide the most assurance of the efficacy of any given study. Further, study efforts by the TO are duplicative, as it is also the responsibility of a TP to identify projects and ensure reliable operation of the BPS years into the future.

The ERO Enterprise finds that the technical rationale provided by registered entities is frequently insufficient to demonstrate compliance with the CIP-014 Requirement R1 risk assessment.²⁶ Audits of CIP-014 frequently do not contain sufficient technical rationale by registered entities that fully supported registered entity decisions and methods for evaluating instability, uncontrolled separation, or Cascading. Sufficient and clear guidance on how to study instability, uncontrolled separation, and Cascading have been available to registered entities in NERC Reliability and Security Guidelines.

From the CMEP Practice Guide for CIP-014-3 R1:

The language within CIP-014-3 does not prescribe a specific method on how each risk assessment of the entity’s Transmission station(s) and Transmission substation(s) shall be performed. As such, specific components that comprise any supporting analytics are neither defined nor listed. This provides intentional flexibility for various approaches to the CIP-014-3 R1 risk assessment, due to the expected differences in each individual entity’s facts and circumstances. However, that flexibility does not alter R1’s language that each risk assessment *must* be “designed to identify” which applicable Transmission station(s) and Transmission substation(s), that if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection. Entities may implement different approaches to complete this objective, but the approach must be able to accomplish the fundamental obligation of requirement through effectively assessing all required adverse system conditions with sufficient supporting technical analyses.

²⁶ NERC CIP-014-2 Peer Review Team – Consensus of CMEP Gap; March 15, 2021.

A recent *Reliability Guideline on the Methods for Establishing IROLS*²⁷ contains the various studies, time domains, and key recommendations to determine the limits substations can take before instability, uncontrolled separation, or Cascading occur. To ensure that no instability occurred in simulation, registered entities can cover each broad type of stability analysis (e.g., frequency or rotor angle) via Contingency analysis, governor power flow analysis, and transient stability analysis; as shown in **Figure 7**. While NERC considers that it would be very difficult for an entity to demonstrate a risk assessment which effectively evaluates instability without performing a dynamics analysis, there is consensus that more specific language to the R1 requirement would add clarity. ERO Enterprise CMEP findings further substantiate that additional clarification in the risk assessment requirement would benefit registered entities in sufficiently assessing instability, uncontrolled separation, or Cascading.

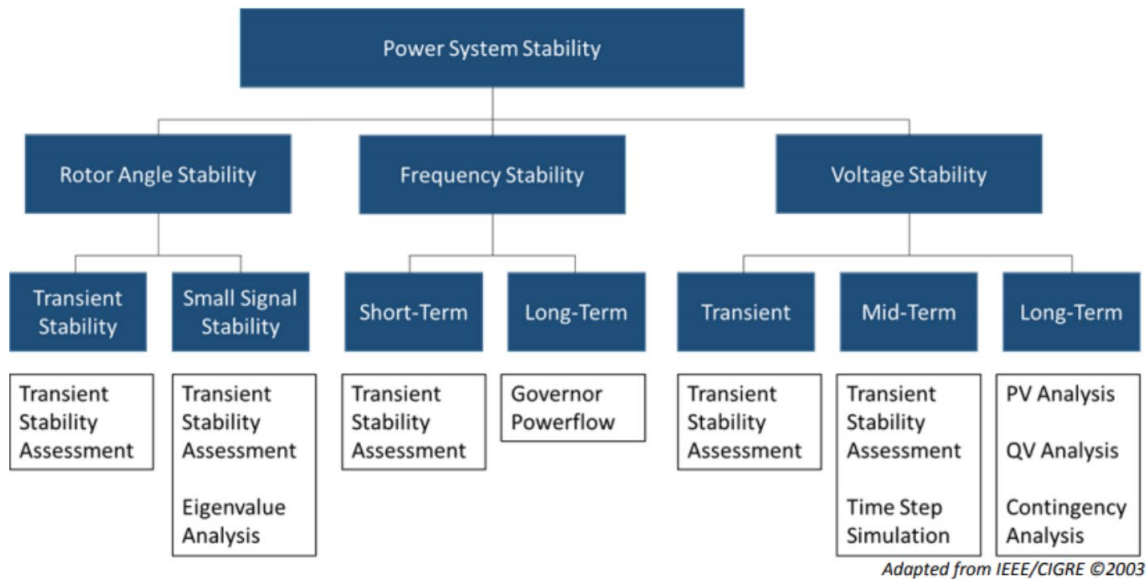


Figure 7: Generic Overview of Power System Stability

The technical rationale included in CIP-014-3 lists a few different example criteria to weigh the electrical impact for a particular Contingency (i.e., the loss of a transmission substation) among which include TPL-001 R6, EOP-004, and impact area. According to the technical justification, the registered entity “has the discretion to choose the specific method that best suites its needs. As an example, a registered entity may perform a Power Flow analysis and stability analysis at a variety of load levels.” The variety of what study criteria may be most appropriate for a registered entity’s facts and circumstances supports the benefits of built-in flexibility in requirement language for the risk assessment. For instance, some registered entities added facilities identified as part of IROL to the potential list of criteria, which carries with it the SOL Methodology found in FAC-014-2.²⁸ However, ERO stakeholders have identified that the variety of criteria used in the risk assessments is not always the most appropriate to effectively evaluate instability, uncontrolled separation, or Cascading. As such, the ERO Enterprise agrees that CIP-014-3’s risk assessment should be clarified in establishing the criteria used in the risk assessment to measure instability, uncontrolled separation, or Cascading.

²⁷ NERC, *Reliability Guideline: Methods for Establishing IROLS* (Sept. 2018), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLS.pdf.

²⁸ Reliability Standard FAC-014-2 – Establish and Communicate System Operating Limits, <https://www.nerc.com/pa/Stand/Reliability%20Standards/FAC-014-2.pdf>.

Severity of Case

Registered entities design risk assessments to be flexible enough to gather the necessary data and perform an analysis that suits its local facilities. However, collaboration with ERO stakeholders have identified that while flexibility covers instances of high stress on the in-scope substations, it is not clear that the risk assessment requires registered entities to use models that correlate to periods of high flows or high stress on their system. Typically, registered entities in the NERC footprint are either winter peaking or summer peaking. These peak conditions historically have been associated with times of higher stress on the transmission system and a higher likelihood that a registered entity reaches its stability margin. As physical security attacks may be planned events, CIP-014-3 risk assessments should seek to evaluate conditions during the most stressed of conditions. Implementing best practices in the case of CIP-014-3 is in line with the standard's purpose and these more potentially severe threats.

Through collaboration with ERO stakeholders, NERC has identified that the term "inoperable or damaged" may leave registered entities too much flexibility when determining study criteria. NERC has verified during multiple oversight activities that registered entities often do not study a more severe failure. Many registered entities have found that the term "inoperable" includes the total loss of communication and protection equipment at the substation, necessitating delayed clearance from far-end relaying to isolate the event's impacts. Damaged substations may be able to self-isolate, and thus would indicate a normal clearing time. Reliance on local relays at the substation that is also under attack should not be permitted. Clarifying this issue could assist in a "worst case" risk assessment versus a design scenario for security professionals to perform a Design Basis Threat ("DBT") analysis to mitigate the "worst case" of the substation being rendered inoperable or damaged.

Physical Proximity Determinations

The CIP-014 R1 risk assessment differs from most other transmission planning studies in that the registered entity must consider physical proximity regardless of electrical connection, as the CIP-014 assessment requires the entire transmission station to be put into an outage rather than just particular elements inside the substation. An example of the type of factors to consider when assessing close proximity is where proximity is defined as having two or more substations situated such that one or more of the following apply:

- An easy line-of-sight between the entire substation yards from a single site.
- An easy access from a common public roadway that exists between all of the substation yards.
- The substation yards are in close enough proximity that a single event can impact both substations (e.g., the debris field from an incendiary device set off at one yard will impact the other yard).

The ERO Enterprise identified areas of concerns in the inconsistent application to determine the proximity of substations for determining CIP-014-3 the assessment. Debates on inclusion or exclusion of this equipment for the Contingency definition typically occur when two or more substations are within eyesight of each other or if they are jointly owned substations. Reliability Standard CIP-014-3 does not set distance requirements or outline other factors for determining whether there is a single substation or multiple substations for applicability or risk assessment purposes. Regional Entity stakeholders agree that there is a need to clarify how registered entities should account for physical proximity when defining the Contingency to input a CIP-014 applicable facility into the R1 risk assessment, such as when substations are within line-of-sight of each other. Registered entities that develop and can demonstrate a consistently implemented method for determining physical proximity would be considered a best practice.

Guidance and training to CMEP staff include evaluating methods used for determining physical proximity issues. CMEP staff may choose to conduct site visits during their fieldwork to substantiate registered entity-applied methods or to perform verification in cases where physical proximity determinations are unclear. NERC recommends that a SAR that clarifies this Contingency definition be included in the enhancements to the R1 risk assessment.

Adequacy of Risk Assessment Criteria Conclusions

As described above, ERO Enterprise CMEP activities indicate that while the overall objective of the Requirement R1 risk assessment is sound, there are inconsistent approaches to the risk assessment. The ERO Enterprise observed that in certain instances registered entities failed to provide sufficient technical studies or justification for study decisions. This has resulted in instances of noncompliance, such as when registered entities were unable to sufficiently substantiate the risk assessment. The inconsistent approach to the requirement is likely impacted by a lack of specificity in the requirement language as to the nature and parameters of the risk assessment.

Given NERC's finding regarding the inconsistent application of the Requirement R1 risk assessment, NERC will initiate a Reliability Standard Development project to evaluate changes to provide additional clarity on the risk assessment. NERC recommends the following:

- Clarify the risk assessment methods for studying instability, uncontrolled separation, and Cascading, such as the expectations of dynamic studies to evaluate for instability.
- Clarify the case(s) used for the assessment to be tailored to the Requirement R1 in-service window and correct any discrepancies between the study period, frequency of study, and the base case a TO uses.
- Clarify the documentation, posting, and usage of known criteria to identify instability, uncontrolled separation, or Cascading occur as part of a risk assessment. The criteria should also include defining "inoperable" or "damaged" substations such that the intent of the risk assessment is clear.
- Clarify the risk assessment to account for adjacent substations of differing ownership, and substations within line-of-sight to each other.
- Clarify that the risk assessment should simulate the complete loss of a Transmission station or Transmission substations that includes the simultaneous loss of all station elements and a does not rely on local system protection for relay clearance.

Evaluation of Minimum Level of Physical Security Protections

As discussed below, while NERC is not recommending an expansion of the CIP-014 Applicability criteria at this time, NERC finds that, given the increase in physical security attacks on BPS substations, there is a need to evaluate additional reliability, resiliency, and security measures designed to mitigate the risks to the BPS associated with physical security attacks. Due to a high degree of public interest regarding physical security following the recent substation attacks, there has been a greater amount of discussion regarding how attacks are mitigated through successful implementation of NERC Reliability Standards. There has also been some confusion regarding some of the discussions points within the public narrative as CIP-014 is inferred to be the measure to prevent all physical attacks and mitigate their associated impacts. This section first discusses the analysis of event data NERC is using in this report and the physical security threat landscape. This information is important to consider when addressing proper security risk assessments.²⁹ Second, this section outlines how physical protections are uniquely designed and implemented to accomplish specific objectives and are not uniform or interchangeable. Third, this section discusses what physical security threats are applicable to CIP-014, which ones are not, and why the distinction is important. Finally, this section concludes our assessment that a determination of any minimum level of protections requires a larger, coordinated, and collaborative effort to mitigate the impact of physical attacks on BPS substations, including those that fall outside of CIP-014 applicability.

Analysis of Physical Security Event Data

To support the evaluation of reported physical security events, E-ISAC SMEs helped outline the threats and risks facing the electric industry, and provided analysis of the supporting data. The E-ISAC collects physical security incidents through a variety channels. The majority of the information received is provided through voluntary means, including E-ISAC Portal posts, direct sharing by members, as well as through government partners. The other type of sharing is through mandatory reporting, which is a U.S. federal government requirement. Mandatory reports are shared with the E-ISAC for situational awareness purposes only.

Known Limits of Event Data

Due to the voluntary nature of information sharing with the E-ISAC, specific details involving potential motives, identification of suspect(s), criticality of substations and other attributes are often unknown. The E-ISAC encourages members to share any security-related information involving their assets or personnel to help ensure the E-ISAC data set is as accurate as possible in order to provide higher accuracy trend analysis on potential emerging threats to the electricity industry. NERC is unable to evaluate these trends beyond what the E-ISAC and industry provide. For instance, while reported physical security events have increased, this is still an incomplete data set. Meaning that NERC is unable to verify the completeness of the data or to what extent any increase in reporting aligns with an increasing number of events. As details of the events were aggregated, more specific information, such as system conditions at the time of the event (e.g., if the system was operating in a stressed state), are often not available.

A variety of different threat actors and violent opportunists will continue to attempt physical attacks on grid infrastructure. These continuing threats are well documented in industry alerts and publications from E-ISAC, DHS / CISA, and others. To address this ongoing threat landscape, E-ISAC members are encouraged to maintain a heightened awareness of suspicious activity around their facilities, and the E-ISAC continues to monitor activity or trends pertinent to the electricity industry, along with changing tactics, techniques, and procedures (TPPs) used by malicious actors against the grid. Based on the fluidity of the current threat environment, the E-ISAC's assessment represent a living analysis that may change and will be updated to reflect any new pertinent developments. The evaluation in this report is thus based on the information available to NERC at this time.

²⁹ Note that these security risk assessments are different from the R1 risk assessment that is focused on the electrical impact rather than the tactics, techniques, and procedures associated with a physical attack.

Types of Physical Events

While there are some known limits to available data, the impacts of evaluated physical security event data represent a period of heightened threat to end-use consumer load. According to a recent analysis conducted by the E-ISAC, the amount of physical security incidents which have resulted in some sort of measurable outage (i.e., loss of end-use consumer load) have increased by 71% since 2021 and 20% since 2020. **Figure 8** shows the quantity of these incidents since 2020. It should be noted that an outage in this trend indicated at least one customer was impacted as a result of the physical security incident. The data show that the rise of events resulting in one or more customers out of service vary in size, scope, and attack vector. Importantly, of the data reviewed, there have been no outages reported from a physical security event that have also adversely impacted the reliable operation of the BPS.

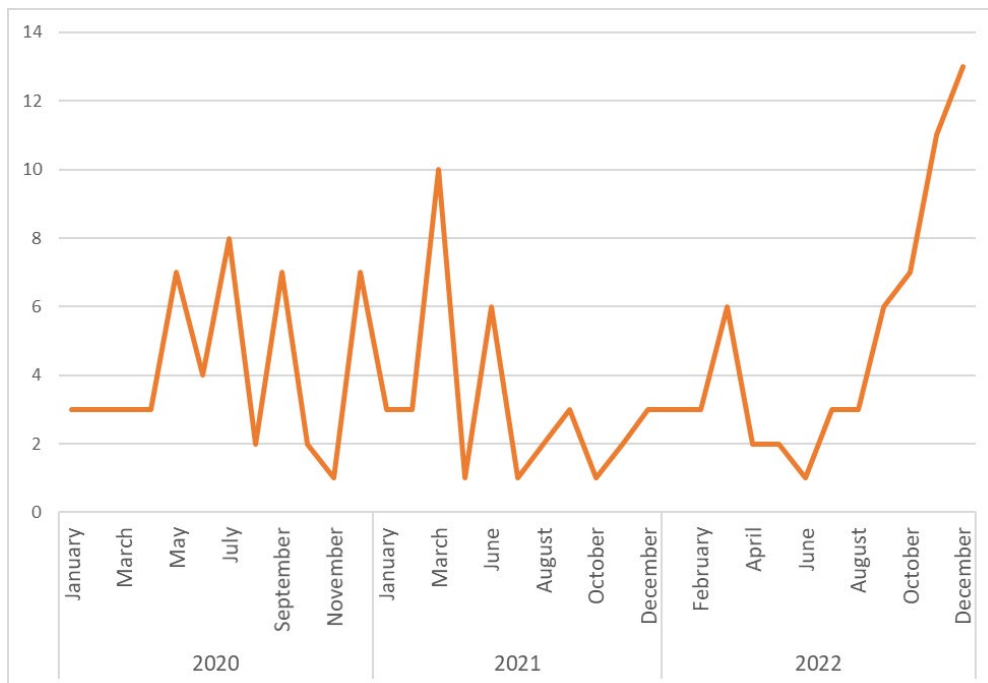


Figure 8: Quantity of Physical Security Events with Some Loss of Load for 2020–2022
[Source: E-ISAC]

The increase in **Figure 8** from 2021 to 2022 is driven by an uptick in ballistic damage, intrusion (tampering), and vandalism incidents. The smaller increase from 2020 to 2022 is due to the high number of reported incidents that occurred during 2020 that can be attributed to the onset of COVID, increased social tensions, and a decline in economic conditions. Of the total amount of physical security incidents shared with the E-ISAC during this timeframe, the vast majority resulted in no disruption to electric service (97%), and the remaining 3% resulted in varying levels of localized impact to end-use consumer load. The impacts of these events vary due the different types of physical threats that occurred as well as the facts and circumstances of the targets, including system topology, system conditions at the time of the event, and other site-specific factors.

A clear understanding of potential impacts from physical attacks is an important aspect of the evaluation in this report as effective protection measures cannot be evaluated without first having a clear objective of what threat and potential impact the security measures are meant to protect against. This data indicates that while there are a number of events corresponding with some loss of end-use consumer load, there are insufficient details to determine the scope of the impact (such as number of impacted end-use consumers over a period of time) and how to project that into potential “worst case” scenarios for that type of threat. NERC is unable to identify from this data what physical security measures were in place at substations that experienced a localized impact nor if any other specific protective measures would have uniformly prevented the impact.

Physical Security Fundamentals

While understanding potential impacts from a physical threat is necessary to outline the objective(s) of new protective measures, not all protective measures are the same or are interchangeable. In order to have a clear basis for what physical security protective measures will be effective at accomplishing the objective, a thorough risk assessment is necessary.

Design Basis Threat Risk Assessments

Physical security subject matter experts agree that risk assessments are a vital first step in determining the effectiveness of physical security measures and associated risk reduction values of those measures. Conducting risk assessments also supports an overall sound risk-management framework, which assists in enabling a structured approach to risk mitigation that can be used by asset owners and operators (“AOOs”). Risk assessments, like that required by CIP-014-3, Requirement R4, also provide assurance of a documented, iterative, and continuous approach to the physical security risk-management process that is critical to the ongoing identification and mitigation of risks.

Realistically, preventing all physical attacks is not feasible when weighed against meaningful risk reduction. Physical security controls that go beyond any identified minimum level of physical security, such as those expected to protect against coordinated or sophisticated attacks on critical infrastructure, should be based on many factors including site criticality, mean time to recovery, and other organization-specific attributes. These factors should be determined through physical security risk assessments to evaluate and define an appropriate selection of physical security protections on a case-by-case basis, as selections appropriate for one site may provide negligible reduction of risk or not be applicable at another. An example of unequal physical protections can be seen by comparing transmission substations versus transmission towers supporting the lines entering that substation. Avenues of approach to a substation are not as varied as those extending along the transmission circuit based on the terrain covered by the circuit impacting the effectiveness of some security controls. These distinctions would be a factor when performing a DBT risk assessment. A DBT risk assessment accounts for the motivations, capabilities, and tactics of potential adversaries who might attempt a physical attack.

Implementation of the Risk Assessment

The E-ISAC’s Physical Security Advisory Group (“PSAG”) developed guidance to provide instruction on using a DBT risk assessment for the protection of the physical infrastructure of the BPS to prevent instability, uncontrolled separation, or Cascading. Methods of implementing a DBT risk assessment, such as Vulnerability of Integrated Security Analysis (“VISA”),³⁰ are available to provide guidance to practitioners.³¹ The VISA method looks at the security functions of detection and assessment, delay, and response, shown in **Figure 9**, and assesses them against a given threat to determine the overall effectiveness of a physical protection system (“PPS”) and to evaluate cost-effective upgrades. To assist in categorizing different types of protective measures, each part of a PPS can be broken down into people, procedures, and equipment.

³⁰ Available on the E-ISAC Portal at: <https://eisac-portal.force.com/eisacportal/s/article/134080-Vulnerability-of-Integrated-Security-Analysis-Implementation-Guide--2021-Update>.

³¹ The threat against which an asset must be protected and upon which the protection system’s design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand.



Figure 9: Three Main Functions of a PPS

Further, ongoing research and design are improving the value of each of these parts with each being an important feature when considering potential upgrades to a registered entity's PPS. Existing resources by the E-ISAC include assistance in the construction of a PPS resulting from the DBT process. These include the recently released *Physical Security Resource Guide for Electricity Asset Owners and Operators*,³² which is available on the E-ISAC portal.

Adaptability by Design

There are a variety of physical security measures, procedures, and actions that asset owners and operators could consider utilizing as part of their operations. As previously discussed, measures are not interchangeable and cannot be expected to provide the same level of protection at all locations or for all threats. Because resources and requirements vary significantly based on a site's size, physical configuration, function, and external factors, implemented physical security protections should be flexible in order to effectively adapt to a changing threat landscape. When determining measures that address asset-specific actions, NERC recommends utilities consult with relevant stakeholder groups, including, but not limited to, management, security, legal, and human resources. In addition, NERC recommends utilities consult relevant authorities, including, but not limited to, laws, regulations, guidelines, corporate protocols, and relevant best practices.

Existing resources, such as the Suggested Protective Measures for Alert Periods,³³ includes suggested adaptive measures that may be implemented during periods of increased alert or threat. These suggested measures represent a compilation from government bodies, private entities, and independent sources and are available for additional consideration when building adaptability into a physical security design process.

Government Mandated Measures

Another factor to consider when identifying what protective measures to incorporate is that industry may be required to include other physical security protections in response to state or Provincial governmental regulation. Recently lawmakers in various U.S. states are proposing regulation to protect substation assets,³⁴ or have already begun implementing these processes in some instances.³⁵ These protections demonstrate that others in the space are working on solutions to address physical security attacks on electric infrastructure. As such, collaboration with

³² Available at: <https://eisac-portal.force.com/eisacportal/s/article/E-ISAC-Physical-Security-Resource-Guide-January-2023>.

³³ Available on the E-ISAC Portal at: <https://eisac-portal.force.com/eisacportal/s/article/127365-Suggested-Protective-Measures-for-Alert-Periods>.

³⁴ For instance, this bill in S.C.: <https://www.scstatehouse.gov/billsearch.php?billnumbers=3577&session=125&summary=B>.

³⁵ Cal. Pub. Utilities Comm'n., Physical Security of Electric Infrastructure (R.15-06-009), <https://www.cpuc.ca.gov/about-cpuc/divisions/safety-policy-division/risk-assessment-and-safety-analytics/physical-security-of-electric-infrastructure>.

government officials will assist in optimizing further proposed requirements and assist in preventing overlapping compliance burdens while still maintaining a strong security posture of the electric ecosystem.

Physical Security Threats and Purpose of CIP-014

This report draws a clear distinction between physical security threats that are considered within the scope of the CIP-014 Reliability Standard and those outside the scope of CIP-014. Each Reliability Standard contains a purpose statement to assist in directing the focus of development and implementation of the Standard. These purpose statements are comprehensive to address a particular risk or set of aggregated similar risks while the Reliability Standard requirements are focused directives in support of that purpose and are each crucial to achieve the Standard's purpose. As previously stated, the purpose of CIP-014 is to identify and protect those substations and their associated control centers that if rendered inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection. CIP-014 intentionally focuses on assuring protections are in place for these critical substations and associated control centers as reliable and secure operation of the Interconnection is paramount to assure all other aspects of NERC's mission are achievable.

Within the Scope of the CIP-014 Purpose

The identification and protection of critical substations and their associated control centers, includes extensive risk assessments, threat assessments, and implementation of resulting plans that provide the highest degree of technical focus and reduction of risk at individual locations. It is unclear that establishing a minimum of physical security protections for critical substations and their associated control centers provides a substantive benefit to reliability as these stations already undergo site-specific threat assessments under CIP-014-3, Requirement R4. Additionally, establishing any specific protective measures may potentially introduce contradicting compliance obligations with the Requirement R4 threat assessment. Further, any potential expansion of the CIP-014 requirements that does not improve upon or close reliability gaps regarding the standard's purpose statement detracts from that goal and may instead reduce the effectiveness of the Reliability Standard overall. Thus, NERC does not recommend modifications to the purpose statement of CIP-014 to address risks posed by the increased number of attacks at non-critical substations.

Outside the Scope of the CIP-014 Purpose

Evaluating whether to extend physical security protection requirements to substations and primary controls outside the scope of CIP-014 necessitates a larger conversation regarding threats and objectives. As outlined in earlier sections, physical security protections cannot be evaluated for potential effectiveness unless they are designed against specific threats, incorporate specific risk reduction objectives, are site-specific, and implemented through an adaptable risk framework. At this time, NERC is unable to make a determination from available data on what set of physical security protections would, if implemented for all BPS substations and control centers, assure prevention or effective mitigation of impacts from recent physical attacks. NERC is also unable to measure the effectiveness or the burden of these measures without identifying first the specific threats or specific risk reduction objectives these controls provide protection against.

Additionally, due to the variability of threats and potential impacts, NERC contends that a focus on only considering physical security protection measures as a means of mitigating the impact of physical attacks on BPS reliability is unnecessarily limited. While minimum requirements for physical security protections may reduce the overall amount of some physical security incidents, establishing a minimum set of uniform protections does not guarantee those protections will prevent outages from sophisticated attacks or equipment by determined bad actors. Other reliability, resiliency, and security measures should be considered for additional operational and planning capability – which could include modifications to existing or new requirements – to assure additional reductions in the potential impacts from physical attacks.

Establishing Minimum Level of Physical Security Protections Conclusions

As noted, requiring a minimum level of protections at all BPS transmission stations and substations and their associated primary control centers necessitates a deeper understanding of the objective of any minimum level of protections, risks the controls should mitigate, and industry resources necessary to meet such minimum requirements. A bright line set of minimum physical security protections, while potentially preventing some forms of attack, does not account for the DBT process nor does it guarantee the protections will safeguard against more sophisticated or coordinated attacks. Effective physical security plans should align with the risks intended to be mitigated. These plans should include responsive or adaptive controls, site-specific attributes, and a viable threat assessment from expert security professionals.

Effective physical security plans include more detail than just protections. As discussed in this report, many physical security controls address a combination of detection, assessment, delay, and response capability. This often means that even a high degree of protective controls are not always intended to completely prevent the occurrence of attacks. The likelihood of some impact becomes more probable the more coordinated or sophisticated the attack as typical deterrence controls become less effective. Any physical security controls that are pursued should be based on many factors including site impact, mean time to recovery, and other organization-specific attributes. These factors should be determined through physical security risk assessments to evaluate and define an appropriate selection of physical security protections. When evaluating the physical security controls for transmission stations, substations, or primary control centers, physical security experts provide technical input on the potential threats, criteria, and solutions. While physical security experts may need to work in concert with other registered entities to identify the electrical impacts of the Facilities, these perspectives are highly important when establishing minimum security controls for all Transmission stations, substations, and their primary control centers. Entities are also encouraged to stay engaged with the E-ISAC and current with posted threat intelligence information and guidance.

Reliability, resiliency, and security measures must be comprehensive in scope, and physical security measures should be weighed against other reliability or resilience measures that cover the same risk. Physical security controls may be an option where registered entities cannot implement other resiliency measures effectively to mitigate the impact of localized outages. While physical security controls may provide some level of assurance against physical attacks from occurring, robust resiliency measures are able to provide long-term adaptability to operations, planning, and security from any type of outage. When outages do occur, invested solutions in response readiness and spare equipment strategies are significant in the reduction of resulting impacts. NERC finds that a combination of reliability, resiliency, and security measures are the most likely to help mitigate the impact of physical attacks on the grid. These combined measures provide increased operational and planning capability as well as improved effectiveness of local network restoration. NERC finds that this more holistic approach will provide greater long-term flexibility and minimize the impacts of physical attacks.

Minimum Reliability, Resiliency, and Security Recommendations

In collaboration with the Regional Entities, there have been many proposed solutions on what constitutes a minimum level of physical security for substations and primary control centers. Further, stakeholders have also shared that BPS elements and distribution substations, if attacked in coordination, constitute an attack vector that can have a significant adverse impact to the BES. Based on the assessment in this report, NERC recommends hosting a Technical Conference to discuss the scope of reliability, resilience, and security measures that are inclusive of a robust, effective, and risk-informed approach to reducing risks.³⁶ The following issues should be considered in the Technical Conference:

³⁶ In some instances reliability-initiated projects can eliminate the security risk, dependent on a myriad of factors. Potentially, these transmission projects can even alter the outcome of CIP-014 risk assessments to identify a critical substation. The Technical Conference proposed should better refine the scope and feasibility of such outcomes for all substations regardless of criticality or configuration and focus on the risk reduction.

Evaluation of Minimum Level of Physical Security Protections

1. The objective of any minimum level of protections, risks to be mitigated, and industry resources necessary to meet such minimum requirements.
2. Expand the use of planning studies to include coordinated security attacks, identify applicable study criteria, and a corrective action plan to mitigate inadequate performance against such criteria as part of their current TPL-001 long-term planning studies.
3. Enhance Operational Planning Assessments to include loss of assets (transmission or generation) from coordinated attacks.
4. Enhance TP and TO requirements to ensure spare equipment pool strategies are adaptive, in-sync, and provide sufficient wide area coverage.
5. RCs develop and train to readiness scenarios reflecting a physical security incident with TOs, TOPs, GOs, and GOPs.

NERC will use the information learned during the Technical Conference described above to determine the next steps, including potential Reliability Standards modifications. NERC plans to consult with FERC staff on the content, timing, and logistics for holding the technical conference. The technical conference on this issue could be held together with or separate from a technical conference on CIP-014 applicability.

Document Content(s)

NERC Report on CIP-014-3.pdf.....1

Plausible Deniability Rather Than Pragmatic Solutions the Signature of NERC CIP

By [Mike T Swearingen](#) – [Originally published on LinkedIn](#)

The Federal Energy Regulatory Commission Inquiries on the Effectiveness of the North American Electric Reliability Standard CIP -014-3

In light of recent physical attacks on the nation's electric grid facilities being brought to the forefront by the media and Cyber threats to the electric grid from Russian and China resulted in a March 23, 2023 hearing by the Senate Committee on Energy and Natural Resources, physical security of the electric grid facilities is considered a new phenomenon. However, for those who have worked within the utility industry, these physical attacks are more common than you may think. The response would naturally be why these incidents over the years have not been reported in the same manner as the recent reports. The simple answer would be the change concerning the physical and cyber security of the electric grid has become more of a political issue due to the increasing importance of the electric grids relation to the ever-increasing critical loads served and the current green energy push. Another answer would be the acknowledged need to more accurately report grid cyber and physical incidents. Further, if one was to examine the reliability indexes reported to the U.S. Energy Information Administration (EIA) and calculate the Average Availability of Service Index (ASAI), an index that provides the percentage of time service is available to consumers, using the EIA information the numbers would reveal pockets within the U.S. where the ASAI percentage is decreasing which is an indication of the increased stress being placed on the electric grid. Given this information it is understandable why the order was issued by the Federal Energy Regulatory Commission (FERC)

On December 15, 2022, the Commission issued Order RD23-2-00 directing the North American Electric Reliability Corporation (NERC) to review CIP-014-3 effectiveness in light of recent physical attacks to electric grid facilities. In the Order, the Commission set forth the following requirements to be reviewed.

- (1) the adequacy of the Applicability criteria set forth in the Physical Security Reliability Standard CIP-014-3 (Physical Security Reliability Standard)*
- (2) the required risk assessment set forth in the Physical Security Reliability Standard*
- (3) whether a minimum level of physical security protections should be required for all Bulk-Power System transmission stations and substations and primary control centers*

On April 14, 2023, NERC issued a report Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System in response to the Commission's Request. The report was intended to answer the questions of the Commission but when reviewed the report reveals less pragmatic and effective solutions and reads more like a legal defense of NERC's current approach and measures. Ironically, the recent physical attacks were on distribution substations that would not be covered by the Order.

NERC CIP-014-3 Standard Exclusivity and the Dangers it Creates

Physical attacks against electric grid infrastructure have occurred for many years causing costly damage and small and even large-scale outages. The question is why the concern now. One of the major arguments is that physical attacks have increased rapidly in recent years but if you were to look at the industry over the past 30-40 years, you would see that physical attacks have occurred on the same scale during that time. Has the grid become more important than it was in the past? The answer would be yes. Due to the advancement of technology and its dependence on the electric grid and the push for green energy the grid has come to the forefront of critical infrastructure of the nation.

It is important to note that NERC operates two sets of standards in the form of operational standards and cyber security and physical standards. The operational standards are based on industry practices of operating the grid over the past 60 years and have their foundation in the electrical properties and physics of electric grid operation. The operational standards have worked well in the operation of the electric grid. Granted changes are made to improve the operational standards due to new and advancing technologies introduced to the electric grid.

In recent years NERC was called upon to develop standards to secure electric grid facilities in the form of the Critical Infrastructure Protection (CIP) standards. The intention of the CIP Standards to protect the electric grid from cyber and physical attacks seemed like a necessary focus to ensure grid reliability and sustainability. However, the issues became apparent when the parameters of the standards excluded the majority of the electric grid infrastructure. This exclusionary practice in the development of the CIP Standards created inherent vulnerabilities that would lead to disruptions in the electric grid.

In the report submitted by NERC on April 14, 2023, the report states that the purpose of CIP-0014-3 is to “identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection”.

The CIP Standard CIP-014-3 is the criteria for the physical security of the electric grid and its critical facilities. When examined the exclusionary nature of the criteria becomes readily apparent. In CIP-014-3 the definition of the facilities covered by the standard is determined by the voltage, above 200kV, and a weighted aggregation of the facilities served by a transmission facility. The argument in support of CIP-014-3 is that the transmission facilities aggregated weight as defined by the standard includes the facilities served. However, this approach focuses on dealing with the transmission facilities without a more refined focus on the facilities connected to it. This causes issues that CIP-014-3 tries to avoid in reducing the risk of large outages due to cascading within the system. An example of the shortfalls within in the standard is one of many I encountered within my long career and a power system engineer.

In this particular case, which occurred 22 years ago, a substation encountered a failure in the 115kV circuit switcher on the source side of the distribution substation. The 115kV circuit switcher failed to operate and remained closed allowing a fault to travel upline to a transmission

interchange causing a large outage. It was determined upon examination that the level of the SF6 arc extinguishing medium was at a level where the circuit switcher did not operate in relation to the ambient temperature at the substation. For those who have worked with circuit switchers the device will not operate if the amount of SF6 in relation to temperature is outside the requirements defined by the manufacturer. The question at first became why the utility was not aware of this condition? At the time the utility did its substation inspection, which is a practice for some utilities, the level of SF6 within the circuit switcher fell within the manufacturer's table of acceptable levels. However, after an inspection it was determined there was a slow leak from the device that occurred between the inspection and when the fault occurred. The cause of the leak was never determined but this is an example of distribution facilities that can cause major outages. This particular substation would be outside the scope of CIP-014-3. It should be noted that this particular substation was interconnected with a looped transmission system. The reason the outage did not cover a larger area was due to a segment of the transmission loop being open at the time. The fact that a segment of the transmission loop was open when it normally operates closed exposes another flaw in the CIP-014-3 requirements since it shows that substations are fed from multiple sources. A condition that is more common than one would think. As a result, the aggregated weight principle for transmission facilities is not sufficient. This is just one of many examples I have seen throughout my career and an example many engineers could relate to.

How CIP-002-5.1a Confines the Requirements of CIP-014-3

While CIP-014-3 has flaws that require changes, CIP-002-5.1 aggregates the problem in the definition of the Bulk Electric System (BES). In CIP-002-5.1a the requirements define BES facilities by underfrequency automatic load shedding (UFLS), undervoltage automatic load shedding (UVLS) of 300 MW or more, the use of Special Protection System (SPS) and Blackstart resources. These requirements exclude a majority of facilities within the electric grid that would be considered as critical infrastructure by Regional Transmission Organizations (RTO), Independent System Operators (ISO) and utilities. This infrastructure that is excluded from the scope of CIP-002-5.1 is contained in the engineering models of RTO's, ISO's and utilities due to how the critical infrastructures function within the system. The reason these facilities are included in the engineering models, would be excluded by CIP-002-5.1a, is because they are a necessary component of the system when evaluating system operation for planning, load flows, protection and the interconnection of new transmission facilities.

When connecting new generation facilities, including renewable energy, the potential interconnection of these facilities must be evaluated in engineering models to determine their impact on the electric grid. In addition, to determine the effect of the generation interconnection not only on a utilities system engineering modeling is required to include the modeling of other interconnected systems. In many cases the inclusion of up-to-date engineering system models of other interconnected facilities requires a request to obtain those models through a Critical Electric Infrastructure Information (CEII) request.

This leads to the question of why CIP-002-5.1a is so exclusionary in its nature. One argument could be made that if you limit the scope of the standard there is a smaller set of facilities you are responsible for. Including all infrastructure would be considered too much of a leviathan for

standard enforcement but being exclusionary presents similar reliability problems because of what is ignored.

The Need for New Solutions to CIP-002-5.1a and CIP-014-3

Based on the current scope of CIP-002-5.1a and CIP-014-3 the grid will face large scale outages due to unrecognized critical facilities. Based on the NERC Report to FERC it appears these issues will remain unresolved.

NERC made the following statement:

NERC acknowledges, however, that supplementary data could show that additional substation configurations would warrant assessment under CIP-014. Accordingly, NERC plans to continue evaluating the adequacy of the Applicability criteria in meeting the objective of CIP-014. Following issuance of this report, NERC will work with FERC staff to hold a technical conference to, among other things, identify the type of substation configurations that should be studied to determine whether any additional substations should be included in the Applicability criteria. The technical conference would also help establish data needs for conducting those studies.

This would seem to be a reasonable statement, but on further scrutiny of the statement made by NERC it can be noted that NERC's evaluation of the adequacy of the applicability criteria within CIP-014-3 would be done in cooperation with FERC staff. While satisfying the requirements of the Commission and its staff is important, NERC should not exclude the input of the industry, especially the input of engineers, technicians and operators of the electric grid.

The report further stated the following:

Clarify the risk assessment methods for studying instability, uncontrolled separation, and Cascading; such as the expectations of dynamic studies to evaluate for instability.

Clarify the case(s) used for the assessment to be tailored to the Requirement R1 in-service window and correct any discrepancies between the study period, frequency of study, and the base case a TO uses.

Clarify the documentation, posting, and usage of known criteria to identify instability, uncontrolled separation, or Cascading as part of the risk assessment. The criteria should also include defining "inoperable" or "damaged" substations such that the intent of the risk assessment is clear.

Clarify the risk assessment to account for adjacent substations of differing ownership, and substations within line-of-sight to each other.

Finally, while NERC is not recommending an expansion of the CIP-014 Applicability criteria at this time, NERC finds that, given the increase in physical security attacks on

BPS substations, there is a need to evaluate additional reliability, resiliency, and security measures designed to mitigate the risks associated with those physical security attacks.

It is important for the Commission and NERC to redefine the criteria of CIP-002-5.1a and CIP-014-3 by developing criteria for critical infrastructure that is defined by the RTO's, ISO's and utilities models which would provide a more accurate account of critical infrastructure. This would provide the Commission and NERC with already established engineering models that could be available for review upon request in any timeline they would consider prudent. However as stated in their report, they are not recommending "an expansion of the CIP-014 Applicability criteria at this time". It seems with all the content contained in the 31-page report submitted by NERC the main takeaway would be that NERC is open to tabletop discussions of potential measures but is currently satisfied with the status quo.

This report, as it stands, is concerning as it continues to allow a vacuum in security that exists through the scope and exclusionary method of standards as currently enforced. Should this trend continue concerning electric grid security and the stress on the grid growing due to the aggressive expansion of green energy without comparable expansion in grid facilities, the nation will be facing a less reliable electric grid and more large-scale outages more frequently.