UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Post-Technical Conference Comments	**)**	
re Physical Security Technical Conference	**)**	**Docket No. RD23-2-000**
under RD23-2 by Secure the Grid Coalition	**)**	

Comments of Secure the Grid Coalition

Submitted to FERC on September 20, 2023

Our Secure the Grid Coalition respectfully suggests that FERC open a Notice of Proposed Rulemaking (NOPR) to modify NERC Standard CIP-014-3. An upgrade of this standard for physical security of the bulk power system is long overdue. This upgrade should, at a minimum, require that the applicability of the standard to substations be based on the system operating and planning models of Regional Transmission Organizations (RTO), Independent System Operators (ISO), Balancing Authorities (BA), Transmission Operators, and other registered entities. These system models are used in daily operations of these utilities and organizations for system monitoring and generation commitments.

Risks To American Public

The American public is now keenly aware of the clear and present danger to the bulk electric system, and thus their lives and livelihoods, from the risk of physical sabotage. The public need not be engineers or grid experts to be able to see with their own eyes just how vulnerable substations and transformers are to attack. Meanwhile, data submitted to the Department of Energy through OE-417s demonstrates that physical attack has resulted in electric disturbances in 1,072 cases from January 2010 through June 2023 – a rate of nearly 1.5 attacks per week (see below). It is just a matter of time before one or more of these attacks results in a major blackout causing immense economic and physical loss. Meanwhile, over the past nine years since approval of CIP-014-1, FERC has declined to order a fundamental overhaul of this obviously ineffective physical security standard despite numerous formal complaints and petitions.

Additions to Factual Record

The recent Joint FERC-NERC Technical Conference on physical security excluded viewpoints dissenting from industry positions. The lack of debate facilitated nonsensical arguments. For example, NERC and

industry panelists exhibited a dualism regarding operating models. As their argument goes, on the "Operations Ledger" the models are vital, but on the "Security/Protection Ledger" the models should not be used to select assets to be protected. Their twisted reasoning says models reliably show which assets, if non-functioning, could lead to uncontrolled separations, cascading outages, or instability—the "evil-three" as they have become known. Yet industry spokespersons argue that they don't want to use these same models to identify which assets are applicable under the CIP standard. The self-contradiction is obvious.

Industry arguments don't stand up in the face of basic scrutiny by the public and they certainly don't stand up in the face of scrutiny by experienced power systems engineers. One such engineer has provided his detailed analysis of the standard as we provide in Enclosure (2).

Enclosure (1) contains a recent letter from our Secure the Grid Coalition co-chairman, former House Speaker Newt Gingrich, to the Chairman of your Commission along with a letter from the former Director of Central intelligence, Ambassador R. James Woolsey – both arguing that your Commission needs to strengthen the physical security standard. We pray that you will do this with haste. Every day that passes without better physical security places the American public in great peril.

Respectfully submitted,

LtCol Thomas J. Waller Jr. (USMC. Ret.)
Co-Director
Secure-the-Grid Coalition
twaller@centerforsecuritypolicy.org

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

Enclosure (1) Letter Requesting Rulemaking for Upgraded Physical Security Standard for BPS
Enclosure (2) Mike Swearingen Letter with Post-Technical Conference Comments

OE-417 Data: January 2010 – June 2023

All NERC Regions		
Events From Jan 2010-June 2023	Total	%
Weather	1250	49.9%
Cyber Attack	56	2.2%
Physical Attack	1072	42.8%
Fuel Supply Deficiency	91	3.6%
Equipment	15	0.6%
Natural Disaster	15	0.6%
Wildfire	5	0.2%
Generation Interruption	22	
Transmission Interruption	192	
Distribution Interruption	9	
Operations	350	
Islanding	67	
Load Shed	31	
Public Appeal	81	
?	11	
Total OE-417 Reports	3267	
Cause Known from OE-417	2504	
Cannot Determine Cause	763	

All NERC Regions															
Event	2023 (through June)	2022	2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011	2010	Total
Weather	39	95	154	162	92	94	80	42	65	82	55	82	133	75	1250
Cyber Attack	3	9	7	7	2	4	3	5	0	3	2	3	8	0	56
Physical Attack	94	166	92	93	80	58	44	49	44	73	79	86	114	0	1072
Fuel Supply Deficiency	1	5	11	7	7	5	7	7	2	18	6	6	6	3	91
Equipment	0	0	0	0	0	0	0	0	0	0	7	2	3	3	15
Natural Disaster	0	0	1	4	0	8	0	0	0	1	0	0	1	0	15
Wildfire	0	0	0	0	0	0	0	0	0	3	0	0	0	2	5
Generation Interruption	0	4	1	0	2	0	4	4	0	0	0	0	7	0	22
Transmission Interruption	14	27	38	42	36	10	9	4	0	0	3	2	2	5	192
Distribution Interruption	0	0	0	0	3	0	0	2	0	1	2	0	1	0	9
Operations	15	76	74	67	56	31	1	16	13	1	0	0	0	0	350
Islanding	0	0	0	0	0	2	1	7	10	15	13	6	4	9	67
Load Shed	0	0	1	0	0	0	0	1	4	2	4	4	5	10	31
Public Appeal	0	8	8	1	0	8	1	4	5	11	0	4	17	14	81
?	1	0	0	0	0	0	0	0	0	4	3	1	0	2	11
Total OE-417 Reports	167	390	387	383	278	220	150	141	143	214	174	196	301	123	3267
Cause Known from OE-417	137	275	265	273	181	169	134	103	111	180	149	179	265	83	2504
Cannot Determine Cause	30	115	122	110	97	51	16	38	32	34	25	17	36	40	763

Secure the Grid Coalition
A Project of the Center for Security Policy
2020 Pennsylvania Avenue, N.W., Suite 189
Washington, D.C. 20006

Enclosure 1

September 18, 2023

Hon. Willie L. Phillips
Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Re: Requested Rulemaking for Upgraded Physical Security Standard for Bulk Power System

Dear Mr. Chairman:

Together with Ambassador R. James Woolsey, I am honorary co-chairman of the Secure the Grid Coalition, which was founded in 2014 by the Center for Security Policy to address the vulnerability of the U.S. electric grid to all hazards. I write today with grave concern about the wholly inadequate physical security of the Bulk Power System (BPS) under your regulatory authority.

As you will see in the attached letter from former Director of Central Intelligence Woolsey addressed to your predecessor over three years ago, our Coalition has been seeking to overcome government and industry inaction that has placed our nation's most critical infrastructure—the electric grid—under threat of attack from terrorists and foreign adversaries.

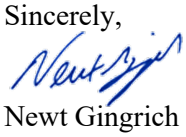
A case in point is the lack of substantive action after Ambassador Woolsey's warning to your Commission about growing physical threats to the grid. In 2020, in connection with Docket EL20-21-000, he wisely called on FERC to review existing reliability standards and direct the North American Electric Reliability Corporation (NERC) to make necessary modifications. Yet, your Commission closed that docket without action. I believe that was a serious mistake.

I am, therefore, heartened that your Commission has shown a renewed willingness to tackle this issue by holding the Joint FERC/NERC Physical Security Technical Conference on August 10th. I pray the end result of that conference will prove to be something other than a pretext for further postponing effective action. It simply must serve as a departure point for improved reliability standards.

Specifically, I urge you to open a Notice of Proposed Rulemaking (NOPR) for an upgrade to NERC Standard CIP-014-3. While adopting this original baseline physical security standard was a modest step forward in 2014, with increasing physical attacks on the electric grid, a reexamination and upgrading of the standard's requirements by your Commission is now absolutely imperative.

The safety and prosperity of our people – and, indeed, the very existence of our nation – depend upon the Federal Energy Regulatory Commission taking prompt regulatory action with an NOPR, rather than engaging in years more of technical conferences and other discussion forums where good intentions are expressed, but few, if any, tangible and meaningful improvements in grid resiliency ensue. We simply cannot afford further irresponsible "business-as-usual" temporizing that, as a practical matter, invites attacks on our most critical of critical infrastructures.

Sincerely,



Newt Gingrich

Secure the Grid Coalition
A Project of the Center for Security Policy
2020 Pennsylvania Avenue, N.W., Suite 189
Washington, D.C. 20006

ENCL 1

March 2, 2020

Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Re: Motion to Intervene in Docket No. EL20-21-000

Dear Chairman Chatterjee and members of the Commission,

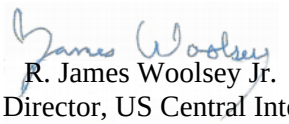
Alongside Former House Speaker Newt Gingrich, I am an honorary co-chairman of the Secure the Grid Coalition, which was founded in 2014 by the Center for Security Policy to address the incredible vulnerabilities of the U.S. electric grid to all hazards.

I have held Presidential appointments in two Republican and two Democratic administrations, served as Director of Central Intelligence, as Ambassador to the Negotiation on Conventional Armed Forces in Europe, as Under Secretary of the Navy, as General Counsel to the U.S. Senate Committee on Armed Services, as Delegate at Large to the U.S. Soviet Strategic Arms Reduction Talks (START) and Nuclear and Space Arms Talks (NST), and as an officer in the U.S. Army. As a senior advisor to the Congressional EMP Commission and as chair of the United States Energy Security Council, I fully recognize that every one of America's 16 critical infrastructures depend upon the U.S. electric grid.

I joined this Secure the Grid Coalition in the wake of a full decade of inaction on the part of government and industry to address the significant threat of EMP to the electric grid, revealed in 2004 by the Congressional EMP Commission. By 2014 we had witnessed, time and again, industry lobbyists work against legislative attempts in Congress to protect the grid. The year prior, in the wake of the sophisticated physical attack on the PG&E Metcalf Substation, we witnessed FERC direct NERC to set a standard for physical security. Effective lobbying by the industry then coerced FERC into exempting all generation plants, most high voltage transformers, transmission lines and the grid's master control rooms from that physical security standard.

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.

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. Recognizing this, I ask that you act with a sense of urgency and draw upon expertise from professionals who specialize in defending electric infrastructure. FERC must review the current standard and direct NERC to make necessary changes in substance and enforcement to update it. Our nation's existence depends upon your Commission getting this right and state regulators following FERC's example.



R. James Woolsey Jr.
Former Director, US Central Intelligence

Enclosure 2

September 18, 2023

Hon. Willie L. Phillips
Chairman
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: Post-Technical Conference Comments for Improving Physical Security Standard for Bulk Electric System

Dear Chairman Phillips and FERC Commissioners,

I am a retired Power System Engineer/IEEE Senior Member with decades of experience. I have prepared, for your consideration, the following paragraphs to illustrate the acknowledged need to combat physical attacks against the Bulk Electric System that occur with greater frequency and with increasing sophistication. I have divided my descriptions and comments into the segments that follow below.

NERC Report to FERC on CIP-014-3 Physical Security and the Technical Conference

The Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) held a technical conference concerning CIP-014-3 Physical Security on August 10, 2023, where selected industry and regulatory officials provided comments and insight on the effectiveness of the standard. This document consists of the comments and analysis of the CIP-014-3 Physical Security Standard and the discussions that took place at the August 10, 2023 Technical Conference.

In NERC's report to FERC, April 14, 2023, the following statements were made:

- *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.*[1]

These statements were further supported by the following statement made by Jamie Calderon, Manager of Standards Development at NERC at the technical conference:

> *In our report, we evaluated the various criteria used in the current version of CIP-014 and found that they were broad enough to cover those substations that would potentially come out during the risk assessment as critical. To be very clear, a large majority of the stations that are considered as applicable, as they meet one or more criteria, are not identified as critical following the risk assessment. There was no indication in our analysis that expanding the list of stations to review within the risk assessment by modifying the criteria, such as lowering the applicable transmission voltages, would find any additional substations that were critical to the Interconnection. The NERC report noted that some additional items could be investigated further, such as modifications from planned system changes – as "as-built" sometimes differ from future plans, but we essentially found that the list of substations being reviewed within the risk assessment were appropriate for identifying those "critical" sites.*[2]

It is clear from the above statements that NERC believed that the selected minimal set of qualifying facilities (brightline) for the Bulk Electric System (BES) are sufficient, if monitored, to avoid instability, uncontrolled separation and cascading, known as the "evil three", of the electric grid.

This approach excluded many facilities that would be found in the system operating and planning models of Regional Transmission Organizations (RTO), Independent System Operators (ISO), Balancing Authorities (BA), utilities and other regional reliability organizations. These system models are used in daily operations of these utilities and organizations for system monitoring and generation commitments and as a result contain all facilities that have a direct effect in ensuring system reliability.

For these reasons, the facilities within the system operating and planning models contain a more accurate account of critical facilities that need to be included in the scope of the CIP standards. Including these critical facilities within the standards are essential to reducing the effect of the "evil three" as defined by NERC.

Development of CIP-014, the History and Purpose of CIP-002, and How These Affect Electric Grid Security

On May 2, 2006, the NERC Board of Trustees approved CIP-002-1 and the standard went into effect June 1, 2006. The original purpose stated in CIP-002-1 was stated in the following manner:

> *"NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."*[3].

Since its original approval and activation as a part of the NERC CIP Standards, CIP-002 has been revised to clarify and define facilities to be included in the Bulk Electric System (BES). The criteria of BES Facilities have been a matter of debate from the inception CIP-002-1 to the current standard of CIP-002-5.1a. This debate is understandable considering that the definition of the BES in CIP-002-5.1a effectively determines the interpretation and compliance of the remaining NERC Standards.

In the current consideration of redefining CIP-0014-3 it is necessary to re-evaluate and redefine the criteria of CIP-002-5.1a.

On October 1, 2015, CIP-014-1 Physical Security became an effective standard in the NERC CIP Standards and has gone through two revisions leading to the current CIP-014-3 Physical Security Standard which became effective on June 16, 2022.

The standard was in response to an order issued by FERC concerning the lack of physical security standard requirements for BES facilities. The purpose of the standard, according to the purpose stated in the 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."* [4]

This purpose is based on what NERC refers to as the "evil three" due to physical attack causing instability, uncontrolled separation, and cascading.

Inadequacies in the Current Version of the Standard

The question is, If NERC considers the evil three something that should be mitigated then why does the standard, by its own requirements, exclude a majority of the facilities that if compromised would lead to the "evil three?"

Comments made at the technical conference and the analysis of this document will outline the inadequacies of the current version of the standard. During the first panel of the Technical Conference Adam Gerstnecker correctly stated that,

> *"The TPL-001 standard does not use an applicability approach like the CIP-014 standard. Instead TPL-001 specifies the types of events to study without narrowing down which substations to examine."* [5]

Adam Gerstnecker stated further,

> *"TPL-001 includes a clearly defined analysis procedure to examine the entire system. CIP-014 does not clearly define the analysis procedure and it only requires a reduced list of substations to be examined. I think CIP-014's applicability section should be eliminated to best identify critical substations based off the results of the analysis of the BES system."*[5].

This analysis so provided by Adam Gerstnecker is consistent with the view of this document, and the Petition for Rulemaking filing of the Secure the Grid Coalition (EL23-69) concerning the use of system operating and planning models which have a more detailed inclusion of critical facilities that need to be covered by the CIP-014 Standard. Because a minimum set of facilities based on voltage and weighted average of facilities is used in the current standard, the use of this method will lead to continued system instability, uncontrolled separation, or cascading within an Interconnection because of the affected facilities that are outside the scope of the standard.

The solution to this obvious impasse is to reassess the standard and change it to the more detailed and inclusive set of facilities based on the system operating models of the Regional Transmission Organizations (RTO), Independent System Operators (ISO), Balancing Authorities (BA), large utilities and other reliability organizations. Based on the comments filed by the Secure the Grid Coalition Docket No. EL23-69-000, FERC's request to review CIP-014-3 in Docket No. RD23-2-000 and comments made at the technical conference on August 10, 2023, it is apparent that the scope of the standard and the criteria within it needs to be changed.

If not changed, and if NERC continues to apply CIP-014-3 and its limited minimal requirements to define critical infrastructure, the mitigation of NERC's "evil three" will continue to be unaddressed in many cases.

System Operation and Planning Models and the Importance of a Complete Set of Critical Infrastructure

In maintaining system operating and planning models NERC has several requirements to ensure the accuracy of the models. Among these are:

- FAC-001-3 Facility Interconnection Requirements,
- FAC-002-3 Facility Interconnection Studies,
- FAC-008-5 Facility Ratings,

- MOD-032-1 Data for Power System Modeling and Analysis,
- MOD-033-2 Study State and Dynamic System Model Validation,
- TOP-002-4 Operations Planning,
- TOP-003-5 Operational Reliability Data,
- TOP-010-1(i) Real Time Reliability Monitoring and Analysis Capabilities, and
- TPL-001-5.1 Transmission System Planning Performance Requirements.

These standards define in detail the facilities and operating data of the grid required for a detailed system operating and planning model. The detail of the system operating and planning models as defined in the listed standards demonstrates the list of critical infrastructure and facilities that must be included for real time system models. This means that within the NERC standards applicable to system operation and planning lies the inherent standards that define a more comprehensive list of critical infrastructure and facilities that need to be referenced in CIP-014 rather than a minimum set of facilities based on voltage and weighted average of facilities.

Another example of the comprehensiveness of the system operations and planning models can be found in Attachment 1 of MOD-032-1 Data for Power System Modeling and Analysis which outlines the facilities and information contained within system operating and planning models which would contribute to a more comprehensive list of critical infrastructure in contrast to the BES requirements of CIP-002-5.1a and CIP-014-3.

Conclusion

In order to properly address physical security of the electric grid it is necessary to remove the minimal set of facilities identified in CIP-002-5.1a and CIP-014-3 and re-write the standards to use the system operating and planning models as defined in FAC-001-3 Facility Interconnection Requirements, FAC-002-3 Facility Interconnection Studies, FAC-008-5 Facility Ratings, MOD-032-1 Data for Power System Modeling and Analysis, MOD-033-2 Study State and Dynamic System Model Validation, TOP-002-4 Operations Planning, TOP-003-5 Operational Reliability Data, TOP-010-1(i) Real Time Reliability Monitoring and Analysis Capabilities and TPL-001-5.1 Transmission System Planning Performance Requirements.

Implementing the revision of CIP-002-5.1a and CIP-014-3 in the manner described in this document would mitigate the frequency of events of instability, uncontrolled separation, and cascading within the electric grid. Importantly, revision to become consistent with these operating and planning models is vital to a multi-dimensional approach required to protect against the more sophisticated “coordinated attack” scenarios, involving simultaneous physical attacks on multiple substations.

_____

Mike Swearingen, Retired Power System Engineer/IEEE Senior Member

References:

[1] Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk-Power System, April 14, 2023, Page 6

[2] Jamie Calderon, Manager of Standards Development at NERC, FERC/NERC CIP-014-3 Physical Security Technical Conference, August 10, 2023

[3] NERC CIP-002-1, June 1,2006

[4] NERC CIP-014-1 Physical Security, October 1, 2015

[5] Adam Gerstnecker, Managing Principal Consultant at Mitsubishi Electric Power Products, Inc., FERC/NERC CIP-014-3 Physical Security Technical Conference, August 10, 2023