UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Physical Security	**)**	**Docket No. RM14-15-000**
Reliability Standard	**)**	

COMMENTS OF THE FOUNDATION FOR RESILIENT SOCIETIES

Submitted to FERC on September 8, 2014

Pursuant to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking (NOPR) issued on July 17, 2014,[1] the Foundation for Resilient Societies, Inc. respectfully submits Comments on the Commission's proposal to approve with modifications Reliability Standard CIP-014-1 of the North American Electric Reliability Corporation (NERC). Our comments consist of the entirety of this filing, including appendices.

The Foundation for Resilient Societies, Inc. (or "Resilient Societies") is incorporated in the State of New Hampshire as a non-profit organization engaged in scientific research and education with the goal of protecting technologically-advanced societies from infrequently occurring natural and man-made disasters. All technologically-advanced societies rely on critical infrastructures—electric power generation and transmission, telecommunications, transportation, financial services, petrochemical refining, food production, water, and sanitation, to name just a few. Sustained interruption of any one of these critical infrastructures can result in economic, political, and social chaos. The profit incentive, which normally serves society well, provides inadequate protection from disasters that occur infrequently but have

[1] Physical Security Reliability Standard, Notice of Proposed Rulemaking, 148 FERC ¶ 61,040 (2014) ("Physical Security NOPR"), issued July 17, 2014.
Fourteen months earlier, and 23 days after the Metcalf Substation attack of April 16, 2013, NERC's RISC Committee unanimously recommended elimination of an under-development standard for Physical Security. The NERC Standards Committee recommended eliminating a physical security standard on June 5, 2013, and the NERC Board eliminated the proposed standard from its work plan in November 2013. Following national publicity in February 2014 concerning the sophisticated attack on the Metcalf Substation in April 2013, the Commission, *sua sponte*, issued an Order on March 7, 2014 requiring NERC's expedited development of a Physical Security reliability standard. See *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

impact beyond the responsibilities of commercial enterprises. The Foundation seeks to identify cost-effective opportunities to protect societies and then develop policy initiatives. Its Board of Directors consists of persons residing in New Hampshire, Arizona, California, Massachusetts, and Virginia. Information about the Foundation may be found at www.resilientsocieties.org.

BACKGROUND

Resilient Societies was an active participant in the NERC Physical Security standard-setting process, both submitting comments and voting as a member of the ballot body. The comments of Resilient Societies in standard setting are included in Appendix 1 to these comments.

Resilient Societies objected to the Standard CIP-014-1 as passed by the ballot body. By letter, we expressed concerns about standard inadequacies to the NERC Board of Trustees prior to the board's meeting to consider and vote on the standard. Our letter and comments to the NERC Board are included as Appendix 2 and Appendix 3, respectively. The NERC Board appropriately considered our objections in a public meeting but nonetheless decided to approve the NERC-proposed standard as passed by the ballot body.

Pursuant to Section 215 regarding Electric Reliability of the Federal Power Act, the Commission now proposes to approve Reliability Standard CIP-014-1 (Physical Security) as just, reasonable, not unduly discriminatory or preferential, and in the public interest. As part of its approval, the Commission proposes to direct NERC to develop two modifications to the physical security Reliability Standard. These two modifications are:

1. Commission proposes to direct NERC to develop a modification to the physical security Reliability Standard to allow "applicable governmental authorities (i.e., the Commission and any other appropriate federal or provincial authorities) to add or subtract facilities from an applicable entity's list of critical facilities under Requirement R1."[2]

[2] NOPR, July 17, 2014, para. 17.

2. The Commission also proposes to direct NERC to modify the physical security Reliability Standard to remove the term "widespread."[3]

The Commission also proposes to direct NERC to make two informational filings:

1. An informational filing within six months of the effective date of a final rule in this proceeding addressing "the possibility that… proposed Reliability Standard CIP-014-1 may not provide physical security for all "High Impact" control centers, as that term is defined in Reliability Standard CIP-002-5.1, necessary for the reliable operation of the Bulk-Power System.

2. An informational filing within one year of the effective date of a final rule addressing "possible resiliency measures that can be taken to maintain the reliable operation of the Bulk-Power System following the loss of critical facilities."[4]

COMMENTS

We support the Commission's original Reliability Directive on physical security issued March 7, 2014. We note, with regret, that the industry's preferred outcome, after receiving bulletins concerning the Metcalf Substation attack, was from May 2013 onwards to have no physical security standard whatsoever. We commend the Commission for issuing its *sua sponte* Order requiring expedited development of Physical Security standards. We further commend the Commission for seeking supplemental authority by which governmental authorities would be enabled to add or subtract specified "critical facilities" including control centers and backup control centers. Governmental authorities may be anticipated to have additional non-public national security information that should enable the Commission, aided by other appropriate government authorities, and that should enable the Canadian Provinces, aided by their government authorities, to seek modifications of the lists of "critical facilities" requiring

[3] Id.
[4] Ibid. para. 18.

physical security standards and protections. Hence, we support the Proposed Physical Security Standards, with FERC's proposed modifications, as a 1st /stage for physical security standards.

However, Resilient Societies considers that Reliability Standard CIP-014-1 as drafted by NERC and as modified by FERC, will inadvertently enlarge the "gap" between the physical security "requirements" for a resilient electric grid and the physical security "capabilities" of that grid in coming years, unless the Commission mandates development of a Phase 2 Physical Security Standard development process.

Without FERC mandate for a Phase 2 Physical Security Standards Development, the Phase 1 standard that FERC proposes to adopt will not be just, reasonable, or in the public interest. The proposed modifications of the Commission, as well as the proposed informational filings, are steps in the right direction, but they will not fully rectify a standard that is fundamentally defective and deficient. However, we recognize that the Commission may nonetheless approve Reliability Standard CIP-014-1 and follow-up with additional Reliability Directives on physical security.

Reliability Standard CIP-014-1 unreasonably exempts whole categories of NERC Registered Entities that are critical to the reliable operation of the Bulk Power System. These entities include:

1. Reliability Coordinators (RCs)
2. Balancing Authorities
3. Generator Operators and Generator Owners

For a detailed rationale for why these entities should be included in the standard's Applicable Entities, see Appendix 1.

The standard does not require modeled contingency planning for scenarios of physical attack. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard.

Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, Midcontinent ISO, and Southwest Power Pool. In all, these three control centers, and three associated backup control centers, manage electric power for over 100 million Americans.

While FERC Directive RD14-6-000 did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Examples of specific physical security requirements that should be considered include:

- **Gunfire Locators.** Gunfire locators, had they been installed at Metcalf Substation, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement.

- **Intentional Electromagnetic Interference (IEMI) Detectors.** IEMI detectors would be another specific security measure that could alert both specific site managers and Bulk Power System operators of hazards that go beyond an attack on a single facility.

- **Automated Intrusion Detection Alarm System Reporting**. Alarms should be reported to Reliability Coordinators, local and state law enforcement, and federal operations centers. One function of effective physical security measures should be to expedite wide-area visibility and reliable rapid response to counter physical attacks before extensive damage is inflicted. We have developed an understanding of the feasibility of automated alarm reporting to multiple recipients – whether the threat is a solar storm or a physical security attack. To avert the concurrent loss of many grid-critical facilities, the automated receipt of near-real-time security alarms could enable: deployment of local law enforcement, state law enforcement, or mobilization of the National Guard.[5]

[5] Press reports indicate that on April 16, 2013 the Santa Clara Sherriff's Department deployed to Metcalf Station, but returned to base without field investigation, after being unable to gain entry to the facility; and only did field

The process for review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans.

For more detail on our comments, please see Appendix 1, Appendix 2, and Appendix 3 of this filing.

SUMMARY CONCLUSIONS

RD14-6-000 directed NERC to submit for approval a physical security standard that would narrowly apply to the most critical facilities of the Bulk Power System. The Standard Drafting Team has unreasonably interpreted "critical facilities" to mean only transmission facilities and directly linked control centers while leaving out facilities that are critical by any reasonable criteria—examples include the control centers for only 16 Reliability Coordinators. If the Commission were to direct a modification of the standard to allow applicable governmental authorities (i.e., the Commission and any other appropriate federal or provincial authorities) to add or subtract facilities from an applicable entity's list of critical facilities under Requirement R1, this is a reasonable stopgap measure. Obvious candidates for added facilities might be:

1. Primary and backup control centers for Peak Reliability, Midcontinent ISO, and Southwest Power Pool—an increase of 6 control centers as compared to approximately 200 already included control centers for Transmission Operators.

2. Nineteen additional Balancing Authorities as compared to 114 Balancing Authorities in total.

---

investigation work after daylight, many hours later. Again, on August 27, 2014, at the same Metcalf Substation, intrusion detection alarms sounded, but these were not reported to the Santa Clara Sherriff's Department, which came to investigate only many hours later, after daylight, with a new shift of security employees. Automated alarm reporting systems, reaching multiple recipients, may be essential to expedite assessment of coordinated multi-site intrusions, and to expedite multi-site protective responses.

3. Approximately 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked.

4. Mandatory intrusion or attack detection and near-real-time reporting systems routed to multiple entities responsible for defense against physical attacks on the Bulk Power System. These entities might include: Reliability Coordinators, local and state law enforcement, and the DOE Operations Center.

These would be marginal additions as compared to the total facilities covered under the standard and therefore would be cost-effective.

For the issue of "High Impact" control centers currently exempted under the standard, the proposed Commission informational filing is a reasonable stopgap measure.

For other gaps in the standard, we ask that the Commission direct NERC to open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of Bulk Power System operations sufficient to ensure identification of facilities that could cause cascading outage and consider single points of failure, data connectivity needs, and other processes and technologies essential to grid protection—in short, a standard designated "CIP-014 Version 2." Such a directive from FERC would be consistent with past practice of the Commission when NERC develops an inadequate standard.

Respectfully submitted by:

Thomas S. Popik, Chairman, and

William R. Harris, Secretary, for the

FOUNDATION FOR RESILIENT SOCIETIES, INC.

52 Technology Way

Nashua, NH 03060-3245

www.resilientssocieties.org

Appendix 1

Comments of Resilient Societies Submitted to NERC in Standard Setting

1. Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 — "System Restoration Coordination"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 — "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 — "Notifications and Information Exchange Between Reliability Coordinators." NERC's own report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded NERC's own report in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.- Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>
2. Balancing Authorities would be exempted under the standard. According to the NERC Compliance Registry, there are 19 Balancing Authorities that are not also Transmission Operators or Owners. The following standards apply to Balancing Authorities but not to Transmission Operators or Owners: Standard BAL-001-2 — "Real Power Balancing Control Performance"; Standard BAL-002-1 — "Disturbance Control Performance"; Standard BAL-003-1 — "Frequency Response and Frequency Bias Setting"; Standard BAL-004-0 — "Time Error Correction"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies"; Standard IRO-006-5 — "Reliability Coordination — Transmission Loading Relief". If critical substations and their Balancing Authorities are attacked in a coordinated manner, what entity will balance demand and generation and manage the emergency, especially if the attack causes a regional load imbalance?
3. Generator Operators would be exempted under the proposed standard. Generator Operators have vulnerable and hard-to-replace Generator Step Up (GSU) Transformers, just as Transmission Operators have these transformers. Generation facilities could present contingencies in excess of spinning reserves, especially in congested areas with import of large megawatts of power over long transmission lines. Hence, Generator Operators should be included in mandatory physical security protection standards.

4. The standard does not require modeled contingency planning for scenarios of physical attack. Contingency planning for physical attack should include megawatt capacity of all generators at single generation facility, not just failure of some individual units at the facility.
5. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard. Physical attack of multiple transformers is different than the random failures planned for under the standard N-1 criterion. We have already seen attack on multiple transformers and their circuits at the Metcalf substation. The standard's criterion for violation of IROL limits would not be valid if the IROL limits assume random failures rather than coordinated physical attack.
6. Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, MISO, and SPP. In all, these control centers manage power for 141 million Americans. Control centers for Reliability Coordinators, Balancing Authorities, and Generator Operators are included in the "High Impact" Criteria for CIP-002-5.1 How can the standard drafting team take the CIP-002-5.1 criteria for substations but not control centers of Reliability Coordinators, Balancing Authorities, and Generator Operators? FERC Directive RD14-6-000 specifically requires protection of critical control centers in Footnote 6: "… the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."
7. While FERC Directive RD14-6-000 [146 FERC ¶61,166] did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Such measures might include: Opaque Fencing; Concrete Jersey Barriers; Motion Sensors; License Plate Scanners; Intentional Electromagnetic Interference (IEMI) Detectors; Gunfire Locators; Limiting of Close Public Access, Including Recreational Access; Armed Private Guards; Police Details; Deployment of National Guard Troops; Better Stocking of Spares—e.g., Transformer Bushings and Radiators; Equipment Monitoring and Redundant Telemetry to Control Centers. Instead, the standard relies upon self-devised security measures without prioritization or other guidance.
8. The Metcalf incident unambiguously showed the value of equipment monitoring in mitigating physical attack on power transformers. Gunfire locators, had they been installed at Metcalf, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement. Intentional Electromagnetic Interference (IEMI) Detectors could likewise provide real-time warning. If threat sensors with reliable and cyber-protected alerts are not part of a physical security system, it will be impossible to mobilize time-urgent countermeasures and impractical to take precautionary measures at other at-risk facilities vulnerable to coordinated attack.
9. Intentional Electromagnetic Interference should be a physical threat included in the standard, because IEMI attack could occur in the physical proximity of facilities and could cause permanent physical damage in additional to temporary upset. IEMI detectors are a cost-effective measure as these devices cost approximately $15,000 per unit.
10. The Metcalf Incident was both a physical attack and a cyber-denial-of-service attack. The need for linkage between physical and cyber is explicitly called for in the RD14-6-000 Order of March

7, 2014, para 5, footnote 3. The implementation plan under this Order must require responsible entities to identify and protect cyber assets that link facilities and control centers that are otherwise identified as critical to the reliability of the BES. Communications and Network entities routinely provide hardened and alternate routing for military, other government and the Defense Industrial Base and their services should be an explicit requirement for Physical Security Standards that apply to any units and control centers that are identified by Responsible Entities as critical to the Reliability of the BES.

11. Review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans.
12. Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP—an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked.
13. RD14-6-000 directs NERC to submit for approval a physical security standard that would apply to the most critical facilities of the Bulk Electric System. The Standard Drafting Team has narrowly interpreted "critical facilities" to mean transmission facilities and directly linked control centers. We disagree with this narrow interpretation. Given the NERC interpretation and the 90 day deadline for standard development, NERC's draft standard holds tightly to the most minimal facilities and therefore has significant gaps in protection as we describe in our foregoing comments. Some of these gaps, such as the exemption of Reliability Coordinators and Balancing Authorities, are so fundamental that they should be addressed immediately. For other gaps, we ask that NERC open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of BES operations sufficient to ensure identification of facilities that could cause cascading outage, single points of failure, data connectivity needs, and other processes and technologies essential to grid protection—in short, a standard designated CIP-014 Version 2. An approved SAR for a Phase Two standard should be concurrent with NERC Board of Trustees approval of the current standard in development.

Appendix 2

COMMENTS OF THE FOUNDATION FOR RESILIENT SOCIETIES ON NERC-REVISED PHYSICAL SECURITY STANDARD CIP-014-1

May 5, 2014

The Foundation for Resilient Societies retains its concern that "critical facilities" should include all Regional Coordinators (RCs) and Balancing Authorities (BAs) and not merely Transmission Owners and Operators. The result of NERC's scaled-back coverage for physical security standards is to leave unprotected RCs and BAs that are not registered as Transmission Owners or Operators. As a result, we estimate that electric power for at least 141 million Americans will not have the relevant Regional Coordinator or Balancing Authority covered by Standard CIP-014-1.

Even for those Transmission Operators covered by the proposed physical security standard, for requirement R3, it appears that only a "primary control center" will be included in the standard requirements. The Metcalf substation assault, for example, was primarily kinetic, but it also constituted an attack on critical communication links. Hence it was a "denial of service" attack that fortunately did not block all instrumentation of overheating transformers available to the primary control center. What are the combined risks of a cybersecurity assault on a primary control center, while a secondary control center is not adequately protected from physical attack? Our Foundation supports physical security standard protection for both primary and backup control centers. This goal is not achieved by the present proposed standard.

The Foundation considers the rationale of the Standard Drafting Team (SDT) for excluding Generator Operators and Generator Owners from a physical security standard to be illogical. The SDT "determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard." We understand that a co-located transmission substation at 500 kV or higher may trigger partial coverage of the facility switchyard, but this coverage may be inadequate.

Why should an ability to detect the loss of high voltage generating facilities justify leaving them unprotected by a physical security standard? Without physical protection standards for major generator facilities, it will be easier for planners of a coordinated attack on selected transmission facilities to also attack generation facilities that operate with self-determined physical security standards. This could aggravate the physical scope or duration of electric blackouts. The physical security requirement for generation facilities in the cyber protection standard is weak and inadequate.

The Foundation does support the proposed exclusion from these (weak) physical security standards for nuclear power plants licensed by the Nuclear Regulatory Commission (NRC). NRC has a record of physical security standard-setting and inspections that will better serve that segment of the electric utility industry.

Finally, we urge NERC and its Board of Trustees to proceed with a Standard Authorization Request (SAR) for a Phase 2 physical security standard-setting. It may have been unrealistic to expect a rigorous standard setting process within a 90-day time limit imposed by FERC. This is not a reason for either NERC or FERC to forego systematic modeling of the bulk electric system, to better determine which facilities and inter-facility linkages require improved physical security standards.

Appendix 3

Foundation for Resilient Societies
52 Technology Way
Nashua NH 03060
www.resilientsocieties.org

May 6, 2014

Frederick W. Gorbet, Chair
Paul F. Barber, Vice Chair
Janice B. Case
Robert G. Clarke
Gerry W. Cauley
David Goulding
Douglas Jaeger
Kenneth G. Peterson
Bruce A. Scherr
Jan Schori
Roy Thilly
Board of Trustees
North American Electric Reliability Corporation
3353 Peachtree Road, N.E. Suite 600, North Tower
Atlanta, GA 30326

Dear Trustees:

Scheduled for your May 7th Board of Trustees meeting is "Agenda Item 8e—Physical Security Standard — Information." We urge you to conduct an independent review of Standard "CIP-014-1 – Physical Security" whose ballot closed at 8pm on May 5th with 93% voting in favor. Should your board be asked to approve this standard on May 7th, we ask that you vote "no" and send the standard back to the NERC Standards Committee for redrafting or, alternatively, vote to conditionally approve with immediate initiation of a Standards Authorization Request (SAR) to address defects in the standard.

Standard CIP-014-1 was drafted in response to Directive RD14-6-000 of the Federal Energy Regulatory Commission (FERC) for Reliability Standards for Physical Security Measures to protect the Bulk Power System against physical attack. This standard as currently drafted is technically defective and inconsistent with previously approved NERC standards. The proposed standard will not adequately protect the American and Canadian public for the following principal reasons:

1. Applicable entities for CIP-104 -1 include only Transmission Owners and Operators but not Reliability Coordinators and Balancing Authorities. Your own board has ratified an extensive system of NERC standards that require certain coordination, balancing, emergency operation, and restoration duties of Reliability Coordinators and Balancing Authorities but not of Transmission Owners and Operators. Standard CIP-104 -1 as

currently drafted obviates the painstakingly designed system of standards approved by your regulator, FERC.

2. The most critical control centers, including those at Reliability Coordinators with wide-area view of the Bulk Power System, would not be covered under the standard. Moreover, no backup control centers would be covered under the standard.
3. Generator Operators would not be covered under the standard. Generator Operators have hard-to-replace Generator Step Up (GSU) transformers just as Transmission Operators and Owners have hard-to-replace transformers. Physical attack on multiple GSU transformers could cause generation losses in excess of spinning reserves and result in cascading outage. For urban areas with sparse local generation and constricted transmission, loss of one or more generation facilities could result in long-term power shortages.
4. Requirements for review and approval of physical security plans are inconsistent with regulation and audit procedures established by NERC and approved by FERC. Reliability Coordinators control the Bulk Power System and Regional Entities audit compliance with NERC standards. But as the standard is drafted, neither of these entities have a required role in review and approval of physical security plans.

We analyzed the NERC compliance registry to see which entities would not be covered under Standard CIP-104 -1 for physical security. We found that three significant Reliability Coordinators–Peak Reliability, Midcontinent Independent System Operator (MISO), and Southwest Power Pool, providing the highest level of grid supervision for 141 million Americans and Canadians–would have no required physical security plans under the standard. For the state of Michigan, its Reliability Coordinator (MISO), No. 1 Balancing Authority (Consumers Energy), No. 2 Balancing Authority (DTE Energy), and all generation facilities within the state would be exempted from the standard.

The final report of the U.S.-Canada Power System Outage Task Force, written as a result of the 2003 Northeast blackout, found that "Failure of the interconnected grid's reliability organizations to provide effective real-time diagnostic support" was a principal cause of the blackout. Yet Standard CIP-014-1 completely exempts the grid's highest level reliability organizations, Reliability Coordinators and Balancing Authorities. Moreover, the report showed that the epicenter of the 2003 blackout was northern Ohio and the adjacent Michigan peninsula. As advocates for the public, we find it simply incredible that the NERC Standard Drafting Team, in apparent zeal to minimize regulation of electric utilities, would ignore the findings of the U.S.-Canada Task Force and once again leave the state of Michigan dangerously exposed to cascading outage.

The actions of the NERC Standard Drafting Team are all the more egregious when one considers that addition of only six primary and backup control centers at three Reliability Coordinators, out of several hundred control centers that might be covered by the standard, would provide vital

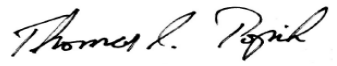
protection for 141 million Americans and Canadians. Surely, the addition of these control centers to the standard's applicability would be cost-effective.

Standard CIP-014-1 with its obvious gaps in coverage provides a roadmap for terrorists and foreign adversaries seeking to attack America and Canada's electric grid. The Metcalf substation attack in San Jose amply demonstrated gaps in physical security for critical grid facilities and their vulnerability to attack. Yet in June 2013, just a few weeks after the Metcalf attack, the NERC Standards Committee voted to cancel the previously approved Standard Authorization Request for a physical security standard. Your board later ratified this cancellation. In the current instance, we ask that the NERC Board of Trustees exercise a higher standard of independent review.

Our organization has participated in the NERC standard-setting process and diligently brought forth our objections to Standard CIP-014-1, but our careful and well researched reasoning was discounted by a Standard Drafting Team dominated by representatives of electric utilities. Attached please find our most recently submitted comments to the Standard Drafting Team.

As independent trustees of NERC, it is your fiduciary duty to conduct a substantive and independent review of Standard CIP-014-1. Again, we urge you to vote "no" on Standard CIP-014-1 because this clearly defective standard would not adequately protect the American and Canadian public from electric grid outages caused by physical attack. Should schedule constraints imposed by FERC preclude outright rejection of Standard CIP-014-1, we ask that a Standard Authorization Request for follow-on physical security measures be drafted and simultaneously approved with any action on Standard CIP-014-1.

Sincerely,



Thomas S. Popik
Chairman, Foundation for Resilient Societies

Attachment: Comments of the Foundation for Resilient Societies on NERC-Revised Physical Security Standard CIP-014-1

cc:
Cheryl LaFleur Acting Chairman, FERC
David Morenoff, Acting General Counsel, FERC