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

| | | |
|---|---|---|
| **Reliability Standard for Revised** | **)** | |
| **Critical Infrastructure Protection** | **)** | **Docket No. RM15-14-000** |
| **Reliability Standards** | **)** | |

# COMMENTS OF THE FOUNDATION FOR RESILIENT SOCIETIES

Submitted to FERC on September 21, 2015

Pursuant to the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking for critical infrastructure protection (CIP) ("CIP NOPR") issued on July 16, 2015, Foundation for Resilient Societies ("Resilient Societies") respectfully submits Comments on the Commission's proposal to approve seven CIP Reliability Standards, to direct the North American Electric Reliability Corporation (NERC) to develop certain modifications to Reliability Standard CIP-006-6, and to develop requirements addressing supply chain management.[1] These Comments are filed solely on behalf of Resilient Societies.[2]

Resilient Societies is a 501(3)(c) non-profit foundation, organized in year 2012, with principal office in Nashua, NH. Resilient Societies engages in research and education to enhance the resiliency of critical infrastructures in the United States and globally.

NERC Standard CIP-014-1 — Physical Security was set in response to a *sua sponte* FERC Order[3] issued after widespread publicity and concern about a leaked FERC engineering analysis. This FERC analysis concluded an attack on only nine critical substations could bring down the U.S.

[1] See *Revised Critical Infrastructure Protection Reliability Standards,* Docket No. RM15-14-000; Notice of Proposed Rulemaking, 152 FERC ¶ 61,054 (July 16, 2015), 80 FR 43354-43367 (July 22, 2015).
[2] Earlier on September 21st, Isologic, LLC and Resilient Societies filed more extensive joint comments in this Docket.
[3] *Reliability Standards for Physical Security Measures*, Docket No. RD14-6-000, 146 FERC ¶ 61,166 (March 7, 2014).

electric grid for over a year. Notably, Standard CIP-014-1 requires physical security for critical substations but places no security requirements on Reliability Coordinators.[4]

Now comes the current CIP NOPR that requires cyber protection of communications among control centers for Reliability Coordinators, but no protection for communications between control centers and substations, including encryption of these communications. If a physical attack on nine substations could bring down the U.S. electric grid, it is logical to conclude that a cyber attack through communications networks for these same nine substations could bring down the grid.

In the Energy Policy Act of 2005, Congress mandated protection of communications networks for the Bulk Power System against cybersecurity incidents.

In July 2015, Lloyd's and the University of Cambridge's Centre for Risk Studies released a report, "Business Blackout: The insurance implications of a cyber attack on the US power grid." The Lloyds' analysis estimated total impact to the US economy of a grid cyber attack at $243 billion, rising to more than $1 trillion in the most extreme scenario.[5]

We investigated the cost of encryption devices for both serial and packet-based communications and found these devices to be both commercially available and cheap. For example, Schweitzer Engineering Laboratories makes "bump-in-the-wire" encryption devices for serial communications (SEL-3021-1 Serial Encrypting Transceiver) that sell for approximately $500 per device, or $1,000 for both ends of a data link. General Dynamics makes widely used encryption devices for packet based communications (TACLANE Micro Network Encryptor) that sell for approximately $10,000 per device, or $20,000 for both ends of a data link.

---

[4] Resilient Societies filed a request for administrative rehearing by FERC on Commission approval of Standard CIP-014-1 for, inter alia, failure of the standard to protect Reliability Coordinators. See (Redacted) Request for Rehearing of FERC Order No. 802 filed in Docket RM14-15-000, Dec. 19, 2014. This request was denied. See FERC Order Denying Rehearing issued April 23, 2015 in Docket RM14-15-001. 151 FERC ¶ 61,066.

[5] "Business Blackout, The insurance implications of a cyber attack on the US power grid," Lloyd's and the Centre for Risk Studies, University of Cambridge, July 2015, available at http://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout. Incorporated in its entirety by reference.

The cost of encryption devices for communication networks serving critical substations appear to be trivial compared to the societal cost of potential outages resulting from cyber attack on the U.S. electric grid.

We respectfully ask the Commission to explain and reconcile the logical inconsistencies in required cyber protection for: Reliability Coordinator Control Centers, other utility company Control Centers, critical substations, and communications networks that interconnect both Control Centers and electric grid substations, across requirements in NERC CIP Standards.

We also ask the Commission to explain why specific provisions of the Energy Policy Act of 2005 for cybersecurity have not yet been implemented, including requiring no specific plans to protect communication networks serving critical substations against cyber attack.

Thomas S. Popik, Chairman

William R. Harris, Secretary,

for the

Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060-3245
www.resilientsocieties.org