UNITED STATES OF AMERICA

BEFORE THE FEDERAL ENERGY REGULATORY COMMISSION

Comments on the Cybersecurity Incentives)
White Paper of the FERC Staff issued June 18, 2020) FERC Docket No. AD20-19-000

Comments of the Foundation for Resilient Societies, Inc. (submitted August 17, 2020)

The Foundation for Resilient Societies, Inc. (hereafter "Resilient Societies"), a 501(c)(3) non-profit research and education organization, commends the Federal Energy Regulatory Commission (hereafter "FERC" or "the Commission") and its Staff for the June 18, 2020 Staff White Paper proposing alternative frameworks and financial incentives to improve cybersecurity of the electric grid.[1] We provide brief comments below:

Question 1: Should the Commission consider adopting one or both of the CIP Reliability Standards and NIST Framework approaches? Describe any other possible approach in detail.

Resilient Societies supports a transition to adoption of the National Institute of Standards and Technology (NIST) Framework as the primary risk-based and mandatory framework for cyber protection of the bulk electric system. We concur in assessments of the Bureau of Reclamation ("Reclamation") filed on August 14, 2020 that the Critical Infrastructure Protection (CIP) standards utilize inconsistent definitions, and we favor adoption of the NIST Framework in place of CIP reliability standards. Our assessment is based in part on the exclusion from "high" or "medium" risk assets of many elements of the bulk power system that are vulnerable to and targeted by foreign cyber adversaries. We also ask the Commission to take notice of the multiple filings in this Docket (and others) by the former Chief Scientist of the National Security Agency, George R. Cotter. Mr. Cotter's detailed analyses demonstrate that electric power flows are generally excluded from CIP reliability standards, while they are a primary target of foreign adversaries. Due to challenges to assure compatibility of the phases, frequencies and voltages of the power grid across regions, CIP standards have excluded tools such as synchrophasors from mandatory encryption or other CIP protections. A shift to 'best practices" incentives within the NIST Framework could facilitate a broader scope for cyber protections, including the protection of cross-regional power flows and the protection of business systems that are target of cyber adversaries.

Question 2: Are the methods for granting incentives based on CIP Reliability Standards adequate?

Resilient Societies does not support financial incentives for CIP Reliability Standards compliance, because we assess the CIP standards to exclude critical assets, including so-called "Low Impact" assets

[1] See Notice of White Paper. Cybersecurity Incentives White Paper. Docket AD20-19-000, issued June 18, 2020.

that are targeted by foreign adversaries, including distribution system assets and vendor-managed software and firmware that can enable cyber adversary takeover of critical grid assets. Resilient Societies could support risk-based cyber incentives across a broader set of grid assets. We also encourage the Commission to consider the proposal of ITC and its subsidiaries, in comments of August 17, 2020, to allow capitalization of some cybersecurity investments, in lieu of a higher rate of return (so-called "adders" to allowable Commission rates) to provide alternative incentives for return on transmission system cybersecurity investments.

Question 3: Should the Commission provide a rebuttable presumption of the reasonableness and applicability of incentives for [CIP Reliability Standard] investments?

Resilient Societies does not support presumptions for rate of return adders based on CIP reliability standards that, overall, do not provide adequate protections from adversary cyber-attack capabilities. Incentives should be based on discernable performance metrics that can be empirically tested, without any presumptions that CIP standard compliance merits rate of return enhancements.

Question 4: Is the proposed approach for granting incentives based on the NIST Framework adequate?

Resilient Societies supports granting incentives based on the NIST Framework, with open ended opportunities for financial incentive if demonstrated on a case by case basis. We also support financial incentives for registered entities that voluntarily report recent cyber incidents and ongoing cyber-attacks to the U.S. government on a near-real-timed basis, for the purposes of supporting (a) cyber deterrence capabilities of the United States, and (b) prompt disruption of cyber-attacks upon electric grid assets, and (c) adoption of sanctions against cyber adversaries and their sponsors.

Question 5: Answer: Any components of the NIST framework should be eligible for cyber protection incentives if demonstrated in cases brought before FERC.

Question 6: Answer: Resilient Societies supports incentives to protect corporate systems, and distribution assets outside the bulk power system, and financial aid to state utility commissions to strengthen cyber protection of the distribution grid.

Federal legislation to aid states' cybersecurity protection, cybersecurity training, and coordination with federal cybersecurity initiative could be beneficial but is beyond the scope of FERC authorities.

Question 11: Answer: A sunset date at some future date might be appropriate to limit consumer charges for existing or future cybersecurity incentives that become obsolete.

Comments are Respectfully Submitted by:

/s/ William R. Harris

William R. Harris,
Director-Emeritus and Attorney
For the Foundation for Resilient Societies, Inc.
24 Front Street
Exeter, NH 03833
www.resilientsocieties.org