FOR IMMEDIATE RELEASE

Federal Ruling on Grid Cyber Regulations Exempts Communications for Critical Substations; Cyber-Hacks on Ukraine Electric Grid Continue after Substation Attacks Cause Major Outage

Nashua, NH—January 25, 2016—Released late last week, a long-awaited federal ruling on cybersecurity regulations for the U.S. electric grid left out protection of communications for critical substations. Meanwhile, cyber-hacking against Ukraine's grid continues after an internet-based attack on grid substations in late December resulted in a major blackout.

In a September 2015 legal filing with the Federal Energy Regulatory Commission (FERC), the federal agency charged with electric grid security, the Foundation for Resilient Societies requested that communications between control centers and critical substations be encrypted or otherwise protected against cyber-attack. Encryption devices costing just a few thousand dollars are commercially available and widely used for military communications; these same devices can be used to protect high-voltage transmission systems. Nonetheless, in its January 21 ruling, FERC determined, "With regard to [Resilient Societies'] argument that the Commission should do more to promote grid security by mandating secure communications between all facilities of the bulk electric system, such as substations, the record in the immediate proceeding does not support such a broad requirement at this time. However, if in the future it becomes evident that such action is warranted, the Commission may revisit this issue."

Ten years after Congress passed a law with the intent of protecting the U.S. electric grid from cyberattack, electric utilities increasingly rely on the public internet for critical communications, including those between grid control rooms and transformer substations. As a result, foreign governments have been able to implant malware into the U.S. electric grid. A May 2013 engineering analysis by FERC, leaked to the Wall Street Journal, determined that an attack on only nine electric grid substations could result in a nationwide blackout lasting over a year.

In October 2014 and again in December 2014, the U.S. Department of Homeland Security (DHS) released alerts informing electric utilities of the risk of infection by "BlackEnergy" malware, reportedly originating in Russia. According to DHS, BlackEnergy malware is capable of taking over electric grid control systems. This same BlackEnergy malware was later used on December 23, 2015 to black out Ukrainian electric grid substations. In Ukraine, cyber-attackers remotely opened breaker switches at grid substations to cause the blackout. In order to restore power, substation switches had to be manually closed by on-site technicians.

The 2003 Northeast Blackout, affecting a population of 55 million from Michigan to New York City, caused Congress to pass a system of mandatory security regulations for the high voltage transmission network of the U.S. electric grid. The Energy Policy Act of 2005 contained specific provisions to require "communication networks" used for the electric grid to be protected against "cybersecurity incidents."

As part of the Energy Policy Act, Congress designed a hybrid regulatory system whereby grid reliability and security regulations would be set and enforced by a private nonprofit

corporation, the North American Electric Reliability Corporation (NERC). Congress also decided grid security regulations would be reviewed and approved by the existing economic regulator of long-distance transmission systems, FERC.

NERC, the private grid regulator, is governed by the vote of its members. Nearly three-quarters of NERC members are representatives of electric utilities. NERC has been slow to develop cybersecurity standards that impose compliance burdens on electric utilities. Under Section 215 of the Federal Power Act, FERC cannot write the text of cybersecurity standards for the electric grid, but can only review and approve the security standards proposed by NERC.

The current version of NERC cybersecurity standards, CIP-005-5, specifically exempts "Cyber Assets associated with *communication networks* and data communication links between discrete Electronic Security Perimeters." (Emphasis added, see page 2.) Instead, so-called "Electronic Security Perimeters," or cybersecurity fences, are established around control centers and grid substations. The cybersecurity standards recently approved by FERC also exempt many electric grid substations used for power distribution from mandatory cyber-protection of any kind.

"The attack against Ukraine's grid clearly shows that substations are a point of cyber-vulnerability," said Thomas Popik, chairman of Resilient Societies. "It's disappointing that the federal agency charged with protecting against catastrophic, long-term blackouts once again put the immediate interests of electric utilities ahead of the mandate of Congress and the security of the American people."

The Foundation for Resilient Societies is a Nashua, New Hampshire-based nonprofit group that performs research and educates on cyber-protection of critical infrastructure. For more information or interviews with critical infrastructure experts, contact Melissa Hancock at media@resilientsocieties.org or telephone 855-688-2430, extension 2. ###.