FOR IMMEDIATE RELEASE

Cyberattack on the Ukrainian Electric Grid Exposes Regulatory Gaps in United States

Nashua, NH—January 11, 2016—A series of cyberattacks on the Ukrainian electric grid, starting on December 23 and continuing for several days, is a stark reminder that a 2005 federal law designed to protect the electric grid in the United States has never been comprehensively implemented. Therefore, America is increasingly vulnerable to foreign cyberattack. Nonetheless, in response to the blackouts in Ukraine, a spokesperson for the quasi-governmental regulator for the U.S. electric grid, the North American Electric Reliability Corporation (NERC), stated, "There is no credible evidence that the incident could affect North American grid operations and no plans to modify existing regulations or guidance based on this incident."

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. Worse yet, no current or proposed federal regulation requires encryption or other cyber-protection of grid communications with substations.

Electric utilities continue to use critical equipment and communications that are inherently not cyber-secure. As a result, the U.S. electric grid remains exposed to potentially devastating cyberattacks. Attackers could damage hard-to-replace equipment, such as large power transformers at grid substations, causing catastrophic long-term blackouts.

In November 2014, the Foundation for Resilient Societies filed a notice on a docket of the Federal Energy Regulatory Commission (FERC) asking that specific cybersecurity provisions of federal law be implemented. FERC is the federal agency ultimately responsible for security of the high voltage portions of the U.S. electric grid. Again in September 2015, in a filing on FERC Docket RM15-14-000, Revised Critical Infrastructure Protection Reliability Standards,-Resilient Societies asked FERC to require cyber-protection of communications between electric grid control rooms and substations. This request to FERC is pending.

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.

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 "communications 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, NERC. Congress also decided grid security regulations would be reviewed and approved by an 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. Newer cybersecurity standards requested by FERC would still exclude many electric grid substations from mandatory cyber-protection.

In Ukraine, cyberattackers 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.

Joseph Weiss, Managing Partner at Applied Control Solutions and an expert on industrial control systems used for electric grids, expressed concern over the Ukraine blackouts and implications for the United States. "The U.S. electric grid and other critical infrastructures are cyber-vulnerable. Many nation-states know that and may already have footholds in our critical infrastructure networks—Russia, China, and possibly even Iran are examples. The NERC Critical Infrastructure Protection (CIP) standards provide compliance to programmatic standards. As the NERC CIPs do not provide actual grid cybersecurity, the NERC CIPs would not have prevented the multiple cyber-related electric outages that have already occurred. Moreover, as the NERC CIP process is public, our enemies are aware of the gaping cyber-holes in our electric grid systems."

The Foundation for Resilient Societies is a Nashua, New Hampshire-based nonprofit group that advocates for 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. ###.