FOR IMMEDIATE RELEASE
Coalition of Infrastructure Experts Calls for Federal Examination of Grid Cyberattack Evidence

Nashua, NH—March 30, 2016—In the wake of the December 2015 cyberattack on the Ukrainian power grid, a coalition of critical infrastructure and cybersecurity experts has called on the Federal Energy Regulatory Commission (FERC) to accept new evidence in its consideration of electric grid cybersecurity standards.

A March 2016 alert by the U.S. Department of Homeland Security confirms pervasive infection of U.S. energy infrastructure with the same family of cyberattack tools used in Ukraine, so-called "BlackEnergy" malware. Globally, security experts have traced the development and use of BlackEnergy to Russia.

On December 23, 2015 a sophisticated cyberattack struck the Ukrainian electric grid, blacking out approximately 225,000 electricity customers. This well-executed attack took over grid operators' control stations, deleted data on hard drives, remotely opened circuit breakers at more than 120 electric substations, and damaged substation equipment necessary for rapid power restoration. Preparation for the attack began over six months earlier with phishing malware allowing the perpetrators to steal grid operators' passwords and other credentials. Indicators of BlackEnergy malware have also been found in Ukrainian mining and railroad companies and in an airport terminal.

Cybersecurity experts have long predicted that a cyberattack can cause a long-term grid blackout and disrupt other critical infrastructure. Events in the Ukraine move the risk of deliberate cyberattack on critical infrastructure from a theoretical possibility to a demonstrated reality.

BlackEnergy malware has been identified in a number of U.S. electric grid penetrations referred to the Industrial Control System Cyber Emergency Response Team of the U.S. Department of Homeland Security (ICS-CERT) since at least 2014. These malware penetrations have received minimal media attention.

In the United States, the electric utility industry and federal regulators have spent the past ten years constructing an elaborate system of cybersecurity standards, officially designated as Critical Infrastructure Protection (CIP) standards. The Ukraine blackout reveals these standards are a false assurance, principally providing liability protection for utilities, but meager protection for the American public. In fact, if Ukraine's electric utilities had followed all of North America's standards for grid cybersecurity, the December cyberattack still would have succeeded.

"The facts and circumstances of the Ukraine cyberattack and resulting blackout are now publicly available in official U.S. government documents, industry studies, and news articles," said Thomas Popik, chairman of Resilient Societies. "Federal regulators can serve the public interest by considering how stricter standards, developed with findings of the Ukraine cyberattack investigations in hand, can better protect the American public from catastrophic blackout."

Significantly, the Ukraine cyberattack demonstrated that a well-planned attack on grid distribution systems—so-called "low-impact cyber assets" under the FERC-approved cybersecurity standards—can cause a high impact blackout. The Ukraine cyberattack by an apparent Russian adversary thus exposes fundamental flaws in the core structure of federal cybersecurity standards that exempt "low impact" facilities. The Ukrainian effort stopped short of physical damage to distribution systems. Had the attackers rapidly switched on and off grid substation circuit breakers, permanent damage to hard-to-replace grid equipment could have occurred, resulting in long-term blackout.

As proof of cybersecurity risks closer to home, there have been several cases where disruption of "low impact" grid equipment has caused large outages. In June 2007, an outage in Phoenix, Arizona affected nearly 100,000 customers and 400 megawatts of load. The April 7, 2015 "low impact" distribution outage in Southern Maryland tripped off the Calvert Cliffs nuclear facility, causing a "high impact" cascading outage that blacked out the Capitol and White House. While neither incident was caused by deliberate bad intent, they highlight the cascading effect of infrastructure vulnerabilities.

"There have been five major cyber-incidents in the United States that resulted in power outages," said Joseph Weiss, managing partner for Applied Control Solutions. "Whether these incidents were malicious or not, they amply demonstrate blackout risks due to cyberattack and the inability of the federal Critical Infrastructure Protection standards to address these incidents."

On March 29, 2016 the Foundation for Resilient Societies, Isologic LLC, and Applied Control Solutions, LLC filed a Request to Reopen the Evidentiary Record at FERC. Resilient Societies is a public interest group with the mission of protecting critical infrastructure against natural and man-made disasters. Isologic is a cybersecurity firm managed by George Cotter, formerly Chief Scientist of the National Security Agency. Applied Control Solutions is a cybersecurity consultancy addressing industrial control systems, including those used in the electric grid.

"Our Joint Motion is an opportunity for the federal government to translate 'lessons learned' from the Ukrainian blackout into defenses against cyber-initiated grid blackouts in North America," said William Harris, attorney for Resilient Societies.

With new evidence, FERC can better determine whether a cyberattack such as demonstrated in Ukraine would place the U.S. electric grid at risk for catastrophic, long-term outage. After consideration of new evidence, FERC may order improvements to cybersecurity standards developed by the electric utility's self-regulatory body, the North America Electric Reliability Corporation. However, under the rules and procedures of FERC, attorneys for electric utilities and their trade associations have the right to file opposing motions asking that evidence of cyberattack vulnerabilities be kept from the public record, possibly ensuring that inadequate grid-protection standards remain unchanged.

For more information or interviews on the coalition's Request to Reopen the Evidentiary Record, contact Melissa Hancock at media@resilientsocieties.org or telephone 855-688-2430, extension 2. ###.