UNITED STATES OF AMERICA
BEFORE THE FEDERAL ENERGY REGULATORY COMMISSION

REQUEST OF THE FOUNDATION FOR RESILIENT SOCIETIES	)	
FOR A MEETING WITH CHAIRMAN CHERYL A. LAFLEUR	)	
SEEKING FERC ISSUANCE OF A *SUA SPONTE* FERC ORDER	)	FERC DOCKET RM13-5-000
TO COMPEL NERC DEFINITION OF "COMMUNICATION NETWORKS"	)	
IN CIP-006-6 AND CIP-007-6 TO COMPLY WITH FERC ORDER 791	)	

November 17, 2014

BACKGROUND INFORMATION

Congress gave the Federal Energy Regulatory Commission (FERC) explicit authority to compel "reliable operation" of the Bulk Power System against "cybersecurity incidents," including disruption of "communication networks." FERC has not implemented these statutory mandates but has only ordered NERC to define "communication networks" as a preliminary step. Now on November 13, 2014 the North American Electric Reliability Corporation (NERC) and its Board of Trustees have openly defied the authority of FERC and refused to define the statutory term "communication networks."

As referenced below, on October 29, 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security released Alert (ICS-ALERT-14-281-01A) "Ongoing Sophisticated Malware Campaign Compromising ICS." This alert, excerpted below, describes malware affecting the GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC software products. These products are used by electric utilities to provide a Human Machine Interface (HMI) for grid operations. For the Cimplicity product, the probable initial infection vector was "a direct connection to the Internet."

Notably, the public Internet is one form of a "communication network." Scans by the Shodan computer search engine have shown numerous electric grid control devices directly connected to the public Internet without use of encryption or other security measures.

As referenced below, on August 8, 2005 Section 215 of the Federal Power Act became law. Section 215 gave FERC authority to approve and enforce reliability standards for reliable operation of the Bulk Power System. FERC was given specific authority over standards for "cybersecurity incidents," defined as "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

As referenced below, on November 22, 2013 FERC issued Order 791 directing NERC to "create a definition of communication networks," see FERC Docket RM13-5-000. Moreover, under the definitions of FERC Order 791, FERC orders that the Bulk Power System be *reliably operated*:

Section 215 (a) Definitions, Para (3) explains that "...reliability standard means a requirement approved by the Commission under this section, to provide for reliable ***operation*** of the bulk power system. The term includes requirements for the ***operation*** of existing bulk power system facilities, including cybersecurity protection,…" (Emphasis added.)

Section 215 (a) Definitions, Para (4) indicates: "The term 'reliable operation' means ***operating*** the elements of the bulk power system…or cascading failures…including a cybersecurity incident..." (Emphasis added.)

Section 215 (a) Definitions, Para (8) defines "cybersecurity incident" as " a malicious act or suspicious event that disrupts or was an attempt to disrupt the ***operation*** of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable ***operation*** of the bulk power system." (Emphasis added.)

The FERC Commissioners should reasonably expect that before the February 3, 2015 deadline, NERC will comply with Order No. 791 and adopt both a definition of "communication networks" and a plan for reliable operation of the bulk power system, including the provision of reliable cybersecurity protection.

Notwithstanding NERC obligations set forth in FERC Order No. 791: on November 13, 2014, the NERC Board of Trustees voted to adopt the Critical Infrastructure Protection Standards Version 5 Revisions, including the associated document, "Consideration of Issues and Directives for FERC Order 791." In this document, the Standards Drafting Team defied FERC Order 791, stating:

1. "The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition."
2. "Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards."

Apparently, NERC seeks to implicitly define "communication networks" as nothing more than nonprogrammable wires and cabling. In contrast, modern communication networks contain programmable aspects such as network interfaces, routers, switches, and encryption devices. Such hardware and software can and must be secured from cybersecurity incidents regardless of whether the communication networks are owned by electric utilities or provided by commercial telecommunications carriers. In fact, it is the programmable nature of modern communication networks that makes them vulnerable to cybersecurity incidents. When Congress enacted Section 215, it well understood that the principal threat to electric grid communications comes not from foreign agents that might lurk around the perimeter of grid

control centers with wire cutters, but from hackers who might attack the grid and its programmable devices from continents away using unsecured communications.

Increasingly, the American public learns of proliferating cyber penetrations of software used to operate the U.S. electric grid. Some malware has reportedly resided within control centers and industrial control systems of the electric grid for more than two years until detection in year 2014. In May 2014, the public learned of the "Ugly Gorilla" cyber threat purportedly by Chinese agents. In July 2014, we learned of the "Energetic Bear" cyber threat purportedly by Russian actors. In October 2014, we become aware of the "BlackEnergy" threat, also purportedly by Russian actors. In each case, the likely attack vector was unsecured Internet communications.

In summary, the Congress enacted a law to protect the public, specifically authorizing "cybersecurity protection" and "reliable operation" of the Bulk Power System. Nine years later, FERC has not implemented the will of Congress, despite explicit authority in Section 215 of the Federal Power Act. On only two occasions since FERC approved an Electric Reliability Organization in 2006 has the Commission issued orders on its own authority (*sua sponte*) to require NERC to develop essential reliability standards: in May 2013 for solar geomagnetic storm mitigation, and in March 2014 for physical security of critical facilities.

Given the gravity and immediacy of the cyber threat to the U.S. electric grid and, by extension, to the American public, the Foundation for Resilient Societies further requests that FERC issue a *sua sponte order* to compel two requirements upon NERC:

1. Develop a definition of "communication network" within 90 days, including programmable aspects of modern communication networks such as protocol implementation, routing, switching, and encryption.
2. Develop an expedited action plan to ensure reliable operation of the Bulk Power System, including initiating reliability standards to protect programmable communication networks against cybersecurity incidents.

Foundation for Resilient Societies respectfully requests a meeting with FERC Chairman LaFleur to discuss cyber threats to the U.S. electric grid, why FERC has not enforced the statutory mandates of Congress, and how FERC intends to deal with the open defiance by NERC and its Board of Trustees.

Submitted by:

Thomas S. Popik
Chairman of the Board
Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060
603-321-1090

Appendix—Excerpts from Relevant Documents

Section 215 of Federal Power Act

(a) Definitions

(3) The term "reliability standard" means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.

(4) The term "reliable operation" means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

(8) The term "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system.

…….

(b) Jurisdiction and applicability

(1) The Commission shall have jurisdiction, within the United States, over the ERO certified by the Commission under subsection (c) of this section, any regional entities, and all users, owners and operators of the bulk-power system, including but not limited to the entities described in section 824 (f) of this title, for purposes of approving reliability standards established under this section and enforcing compliance with this section. All users, owners and operators of the bulk-power system shall comply with reliability standards that take effect under this section.

FERC Order No. 791, Paragraph 150

We direct NERC to create a definition of communication networks and to develop new or modified Reliability Standards to address the reliability gap discussed above. The definition of communications networks should define what equipment and components should be protected, in light of the statutory inclusion of communication networks for the reliable operation of the Bulk-Power System. The new or modified Reliability Standards should require appropriate and reasonable controls to protect the nonprogrammable aspects of communication networks. The Commission directs NERC to submit these modifications for Commission approval within one year from the effective date of this final rule. We also direct Commission staff to include this issue in the staff-led technical conference discussed herein.

NERC Consideration of Issues and Directives for FERC Order 791, October 28, 2014

The proposed CIP-006-6 Requirement Part 1.10 requires the physical protection of nonprogrammable components of BES Cyber Systems existing outside of the PSP, and the proposed modifications to CIP-007-6 Requirement Part 1.2 include applicability for non-programmable electronic components to prevent unauthorized use of physical ports. These additional

requirements address the gap in protection as discussed in the Order by ensuring the physical security for cabling and non-programmable network components not covered by the definition of Cyber Asset.

The drafting team reviewed the directives related to submitting a definition for communication network and determined it could address the gap in protection and adequately provide guidance on nonprogrammable electronic components without having a definition. Communication networks can and should be defined broadly. For example, NIST Special Publication 800-53 Revision 4 refers to the CNSSI 4009 definition of Network, which is "Information system(s) implemented with a collection of interconnected components." The requirements modifications as well as the existing requirements have more targeted components. Consequently, there is not a need at this time to submit a definition for the NERC Glossary of Terms used in Reliability Standards.

ICS-ALERT-14-281-01A

Ongoing Sophisticated Malware Campaign Compromising ICS (Update A)

Original release date: October 29, 2014 | Last revised: November 03, 2014

SUMMARY

This alert update is a follow-up to the original NCCIC/ICS-CERT Alert titled ICS-ALERT-14-281-01 Ongoing Sophisticated Malware Campaign Compromising ICS that was published October 28, 2014, on the ICS-CERT web site.

ICS-CERT has identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs).

ICS-CERT originally published information and technical indicators about this campaign in a TLP Amber alert (ICS-ALERT-14-281-01P) that was released to the US-CERT secure portal[a] on October 8, 2014, and updated on October 17, 2014. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov.

DETAILS

ICS-CERT has determined that users of HMI products from various vendors have been targeted in this campaign, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC. It is currently unknown whether other vendor's products have also been targeted. ICS-CERT is working with the involved vendors to evaluate this activity and also notify their users of the linkages to this campaign.

At this time, ICS-CERT has not identified any attempts to damage, modify, or otherwise disrupt the victim systems' control processes. ICS-CERT has not been able to verify if the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims.

In addition, public reports[b,c] reference a BlackEnergy-based campaign against a variety of overseas targets leveraging vulnerability CVE-2014-4114[d] (affecting Microsoft Windows and Windows Server 2008 and 2012). ICS-CERT has not observed the use of this vulnerability to target control system

environments. However, analysis of the technical findings in the two report shows linkages in the shared command and control infrastructure between the campaigns, suggesting both are part of a broader campaign by the same threat actor.

ICS-CERT strongly encourages asset owners and operators to look for signs of compromise within their control systems environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

CIMPLICITY

ICS-CERT analysis has identified the probable initial infection vector for systems running GE's Cimplicity HMI with a direct connection to the Internet. Analysis of victim system artifacts has determined that the actors have been exploiting a vulnerability in GE's Cimplicity HMI product since at least January 2012. The vulnerability, CVE-2014-0751, was published in ICS-CERT advisory ICSA-14-023-01 on January 23, 2014. Guidance for remediation was published to the GE IP portal in December 2013.[e] GE has also released a statement about this campaign on the GE security web site.[f]

Using this vulnerability, attackers were able to have the HMI server execute a malicious .cim file [Cimplicity screen file] hosted on an attacker-controlled server.