UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Security Incident Reporting	**)**	**Docket No. RM18-2-000**
Reliability Standards	**)**	**Docket No. AD17-9-000**

COMMENTS OF THE FOUNDATION FOR RESILIENT SOCIETIES

Submitted to FERC on February 26, 2018

As initiator of this proceeding, by means of our Petition for Rulemaking filed with the Commission on January 13, 2017,[1] Resilient Societies appreciates the opportunity to comment on the subsequent Notice of Proposed Rulemaking (or "NOPR"), entitled "Cyber Security Incident Reporting Reliability Standards" and proposed by the Federal Energy Regulatory Commission ("FERC" or the "Commission") on December 21, 2017 in FERC Docket No. RM18-2-000.[2]

Background on Foundation for Resilient Societies

The Foundation for Resilient Societies, Inc. (or "Resilient Societies") is a 501(c)(3) non-profit organization engaged in scientific research and education to protect technologically-advanced societies from infrequently occurring natural and man-made disasters. With recognized policy and technical expertise in the use of federal and state regulations to protect electric grids from cyberattack, physical attack, solar storms, and electromagnetic pulse, our group is regularly asked to appear before official government bodies and industry forums. We have testified before the FERC, the Senate National Security and Defence Committee of the Canadian Parliament, and the U.S. House Committee on Oversight and Government Reform. We have deep expertise in the risks of long-term blackout and potential regulatory solutions, having made over two dozen filings in the reliability dockets at FERC and the Nuclear Regulatory Commission (NRC). Media sources such as the *Wall Street Journal, The Economist, Politico, USA*

[1] Petition for Rulemaking to require an enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk Power System, 82 FR 9034-9035 (2017).
[2] 161 FERC ¶ 61,291, 82 FR 61499-61505 (2017).

Today, Reuters, NBC, and Fox News rely on our knowledge of critical infrastructure threats and cost-effective protections.

Summary of Cybersecurity Threats to the U.S. Electric Grid

In the 21st century, nations use threats against the infrastructure of other nations as instruments of power and as a means to deter attacks against their own country. Because electric grids are the keystone infrastructure, upon which all other infrastructures depend, electric grids are primary targets. Cyberattack is a preferred means of infrastructure attack, because it can be executed remotely, with minimal deployment of humans at physical risk. Because fewer resources are needed to execute a cyberattack, as compared to attack with conventional forces, it is an asymmetric and growing threat.

In November 2014, in testimony before the U.S. Congress, then-NSA Director Admiral Michael Rogers admitted that multiple foreign powers have the ability to take down the U.S. electric grid.[3] In February 2017, the Defense Science Board concluded that "limited U.S. efforts to defend U.S. information systems" make it impossible in the foreseeable future "to deny highly capable actors the ability to conduct catastrophic cyber attacks on the United States." In February 2018, the Office of the Secretary of Defense stated in its Nuclear Posture Review that the United States should posture its nuclear capabilities to hedge against non-nuclear strategic threats, including cyber aggression.[4] With weak cybersecurity protections for the U.S. electric grid, America is now forced to threaten first use of nuclear weapons as a deterrent to attack.

Gaps in Current NERC Cybersecurity Standards

We respectfully observe that hundreds of pages of cybersecurity standards proposed by NERC and approved by FERC have not been effective in mitigating strategic cyberattack threats, according to the head of the National Security Agency and the Defense Science Board. Why?

---

[3] Crawford, Jamie. "The U.S. government thinks China could take down the power grid," CNN. (November 21, 2014). Available at: https://www.cnn.com/2014/11/20/politics/nsa-china-power-grid/index.html

[4] Office of the Secretary of Defense. "Nuclear Posture Review" Report. (February 2018). p. 38. Available at: https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

Because NERC and its managers have incentives to set reliability standards that minimize compliance costs for the electric utilities. Representatives of electric utilities make up a super-majority of NERC membership and dominate its key governing bodies. Too often in the past, FERC Commissioners have acquiesced when NERC has proposed weak cybersecurity standards. Moreover, FERC has repeatedly recertified NERC as the designated "Electric Reliability Organization (ERO)." The electric industry is, de facto, the principal self-regulated industry in the United States. [5]

Gaps in NERC's cybersecurity standards are both pervasive and difficult for those outside the electric utility industry to ascertain. For example, so-called "low-impact" facilities are exempted from standards, even though attacks on high-impact facilities can be executed using low-impact facilities as the entry points. Furthermore, a simultaneous attack on several low-impact facilities can have a greater impact than a single attack on a "high-impact" facility. As another example, only a small fraction of the computer systems of electric utilities are covered under NERC's cybersecurity standards—those systems that control high voltage operations of the "bulk electric system": generation plants, switching substations, and control rooms. However, the business computer systems of electric utilities – used for accounting, personnel management, email, web browsing and the like – are connected to the public internet and therefore accessible to cyberattack teams around the world. Many U.S. electric utilities have electronically linked their operational systems to their business systems, thereby extending cyberattack vulnerabilities to computers that control the flow of power to homes and businesses.

[5] See also the comments submitted by Isologic, LLC in this Docket, prepared by the former chief scientist at the National Security Agency, George R. Cotter, a national expert on vulnerabilities of electric grids globally. Mr. Cotter asserts: "CIP Standards have simply failed to protect the Bulk Electric System and therefore the Distribution System, and therefore the infrastructures, institutions, and citizens nearly totally dependent upon the National Grid. Since 2012, Russia has conducted operations against the Grid, performed reconnaissance, collecting intelligence, and developing systematic attack systems…." The Isologic comments observe "The complete absence of an integrated Grid-wide capability to detect Attacks aimed at disabling or capturing a variety of local, regional or national targets represents a vulnerability of staggering proportions. How do Cyber Command and State National Guards respond?...FERC should require development and institutionalization of a nation-wide Situational Awareness structure; if the FPA [Federal Power Act] is a hindrance, Congress can amend the act." Isologic explains: "What is feasible is that a cybersecurity infrastructure across electric utilities (including Distribution assets) be put in place, a reasonable situational awareness program be established nation-wide, and realistic security standards and procedures be developed and enforced." For specific cybersecurity vulnerabilities and regulatory gaps, see the full Isologic comments filed in Docket RM18-2-000 on Feb. 6, 2018.

Occasionally, a gap in the NERC cybersecurity standards is obvious even to lay people and this self-regulatory organization will admit a problem. Such is the case with the current NERC standard for cybersecurity incident reporting. After zero cybersecurity incidents were reported for all of 2015, Resilient Societies urged the NERC Board of Trustees to address "materially misleading statements in regard to the number of reportable cybersecurity incidents" in their annual *State of Reliability* report.[6] While the NERC Trustees did slightly modify wording in their reports, NERC still allowed zero cybersecurity incidents to be reported in the subsequent year, 2016. During the same period, 2015 and 2016, the Defense Science Board, using information on electric grid cyberattacks that have gone unreported by utilities, concluded that grid cyber vulnerabilities are so severe they cannot be effectively defended against "in the near- to mid-term." [7]

In our experience from six years of observation of NERC standard-setting, when FERC proposes a remedy for a gap in reliability standards, NERC can often find a way to exempt significant numbers of electric utilities from taking protective action, even if an "improved" reliability standard is set.[8] The current proposal to require cybersecurity incident reporting only for compromise, or attempted compromise, of so-called "Electronic Security Perimeters" (ESP) and "Electronic Access Control or Monitoring Systems" (EACMS) is no exception. The FERC-proposed reporting threshold would give the NERC Standard Drafting Team wide latitude to craft ways that cybersecurity incidents need not be "reportable." Moreover, this threshold would clearly exempt electric utilities from reporting one of the greatest cybersecurity threats they face — insertion of malware into their business systems. When malware is present in business systems, it can then be used by cyber-attackers as a jumping-off point for attacks into operational systems, as the successful 2015 cyberattacks against utilities in Ukraine conclusively

[6] See Appendix 1 of this comment, containing the text of the May 12, 2016 Resilient Societies letter to the NERC Board of Trustees.

[7] The NERC "State of Reliability Report" with 2017 reported cybersecurity incidents will not be released until summer of 2018, but we expect the number of incidents for this past year to once again understate the true threat.

[8] For example, see Order No. 802, Physical Security Reliability Standard, 149 FERC ¶ 61,140 (Nov. 20, 2014), para. 91, 92 (NERC recommended exclusion of generators, accepted in FERC Order); para. 93 (NOPR excludes generators from physical security requirements); para. 99. As another example, under NERC Standard TPL-007-1, "Transmission System Planned Performance for Geomagnetic Disturbance Events," every transmission substation in the U.S. is effectively exempted from hardware protection by imprudent setting of the Benchmark GMD Event, combined with a high level of assumed transformer withstand to Geomagnetically Induced Currents.

showed. Malware infecting business systems can lay dormant, not even "attempting to compromise" Electronic Security Perimeters and their firewalls protecting operational systems.

Without care by the FERC Commissioners, the new standard developed in response to the December 21st FERC NOPR could minimize and delay reporting of cybersecurity incidents. Without care by the FERC Commissioners, fragmentary and incomplete cyber incident reporting will inappropriately diminish incentives for malware detection and removal. With minimal incident reporting, utilities will have less incentive for Red Team field testing and other "best practices" cyber-threat mitigation programs.

In our comments for this rulemaking, we cannot overemphasize this fundamental observation—the modifications proposed by FERC for mandatory cyber incident reporting will not require reporting of malware that is capable of causing widespread grid blackouts. As a result, the American public will remain at risk, unless the final ruling by FERC has substantial changes as compared to the December 21st Notice of Proposed Rulemaking (NOPR).

Based on six years of experience in FERC rulemaking for reliability standards to protect against high-impact events, we observe the final orders of the Commission generally conform closely to the requirements in the preceding NOPR. Comments from public stakeholders may be given *pro forma* consideration in the final ruling, but will often be placed aside in favor of the "solution" apparently negotiated between FERC and NERC. [9] Should the Commission once again decide to follow this path, we have this concern: *after NERC sets a new standard for cybersecurity incident reporting, and FERC approves the standard, there will still be minimal public reporting of cybersecurity incidents. Potential attackers will most often avoid breaching Electronic Security Perimeters until a full-scale attack is underway. The government, and the public, will lack a true picture of cybersecurity risks for the electric grid and this will prevent the societal consensus necessary for real protection to be implemented.*

[9] Based on a report that is now several years old, it is our understanding that FERC and NERC have a longstanding practice of holding quarterly, non-public meetings to discuss, *inter alia*, the status of reliability standards, including standards in development. Minutes of these quarterly meetings are withheld from public release by FERC. Such meetings give the impression of impropriety, especially when FERC-approved standards minimize compliance burdens but do not effectively protect the public against blackouts. We respectfully ask that the Commission open any regularly scheduled meetings with NERC to other public stakeholders and promptly release for public accessibility the minutes of all prior closed NERC-FERC meetings.

Report of the Defense Science Board

In February 2017, the Defense Science Board completed a two-year study on cyberattack deterrence, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence." In its report, the Board recognized that HAVEX and BlackEnergy malware have been discovered at U.S. electric utilities and concluded:[10]

> Although accelerating improvements to cyber defenses and resilience is vital to strengthen the U.S. posture and provide an essential foundation for deterrence by cost imposition, it will not be possible (for the foreseeable future) to deny highly capable actors the ability to conduct catastrophic cyber attacks on the United States. This is primarily because the limited U.S. efforts to defend U.S. information systems to date are unlikely to accelerate (in the near- to mid-term at least) to the point where they can offset the combination of major powers' technical wherewithal, vast supply of resources (including a supporting intelligence apparatus), and the ability to influence supply chains and exploit vulnerabilities at scale.
>
> However, the United States could – and must – aim to deny North Korea and Iran the ability to undertake catastrophic attacks on U.S. critical infrastructure via cyber, just as the United States aims to deny them the ability to attack with nuclear weapons.

During the same two years of the Defense Science Board study (2015 and 2016), U.S. electric utilities reported zero cybersecurity incidents under the standards of the North American Electric Reliability Corporation (NERC).

Report of the Council of Economic Advisers

The Council of Economic Advisers concluded in its February 16, 2018 report, "The Cost of Malicious Cyber Activity to the U.S. Economy," that the private sector has incentives to underinvest in cybersecurity, while cyberattack costs to the public could be enormous:[11]

> Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. *Failure to account for these negative*

[10] Defense Science Board Task Force on Cyber Deterrence, "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence." Report. (February 2017) Available at: https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf

[11] The Council of Economic Advisers, Executive Office of the President. "The Cost of Malicious Cyber Activity to the U.S. Economy." Report. February 2018. p. 1, 41, 42. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

> *externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment.*
>
> A cyberattack on the electrical grid could have large-scale economic impacts as infrastructure damages, loss in output, delayed production, spoiled inventory, and loss of wages all decrease productivity and earnings for the duration of the blackout.
>
> In addition to the economic impacts of a large power outage, there are health and safety concerns. Power outages impacting heating and cooling systems, at home health systems, refrigeration, and slower emergency response will all increase the rate of illnesses and death in the impacted areas. People will suffer from heat related conditions (such as heat stroke) and hypothermia, spoiled food, and difficulty of emergency responders to communicate with those impacted. In addition, riots, looting, and arson attacks as well as lack of lighting and overstretched police will increase crimes and decrease safety. (Emphasis added.)

Congress recognized the divergence between private sector economic incentives and the need for public protection when it mandated that FERC approve reliability standards "in the public interest." However, under NERC standard-setting practices that minimize compliance burdens, utility investment in cybersecurity has been minimized to the detriment of the public interest.

New Information on Cyberattacks Targeting Electric Utilities

New information has come to light since the February 2017 closure of the comment period for Docket AD17-9-000 for the original rulemaking. Multiple credible sources report cyberattacks recently targeting electric utilities.

A June 12, 2017 article in USA Today, "Malware discovered that could threaten electrical grid," revealed a new variant of malware, "Industroyer":[12]

> A new malware variant capable of knocking out networks that run power grids around the globe has been discovered by a computer security company studying an attack on the Ukrainian power grid.
>
> The malicious code is capable of directly controlling electricity substation switches and circuit breakers and could potentially be used to turn off power distribution or to

[12] Weise, Elizabeth. "Malware discovered that could threaten electrical grid," USA Today. (June 12, 2017). Available at: https://www.usatoday.com/story/tech/news/2017/06/12/malware-discovered-could-threaten-electrical-grid/102775998/

> physically damage equipment used in the electricity distribution grid, researchers at ESET wrote in a paper posted Monday.
>
> Two things stand out about the malware, dubbed "Industroyer" by the researchers — it's an order of magnitude easier to use than previous programs and it wasn't actually deployed to do any real damage, meaning whoever's behind the December attack might simply have been testing the waters.

A September 6, 2017 article in *Wired* magazine, "Hackers Gain Direct Access to U.S. Power Grid Controls," states that Symantec has detected a campaign of cyberattacks and intrusions at U.S. power firms:[13]

> Symantec on Wednesday revealed a new campaign of attacks by a group it is calling Dragonfly 2.0, which it says targeted dozens of energy companies in the spring and summer of this year. In more than 20 cases, Symantec says the hackers successfully gained access to the target companies' networks. And at a handful of US power firms and at least one company in Turkey—none of which Symantec will name—their forensic analysis found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses.
>
> Those attacks were designed to harvest credentials from victims and gain remote access to their machines. And in the most successful of those cases, including several instances in the US and one in Turkey, the attackers penetrated deep enough to screenshot the actual control panels for their targets' grid operations—what Symantec believes was a final step in positioning themselves to sabotage those systems at will.

A September 7, 2017 article in *USA Today*, "Intrusion - but no attack - on U.S. energy grid is a warning, says former NSA official," gave additional details on compromised operational systems:[14]

> Over the last nine months, dozens of U.S. power companies were compromised by an organized hacking group to the extent that some of them could have sabotaged and shut down production and distribution, according to Symantec, a cybersecurity company that discovered the attack.

---

[13] Greenberg, Andy. "Hackers Gain Direct Access to U.S. Power Grid Controls, "*Wired*. (September 6, 2017) Available at https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/

[14] Weise, Elizabeth. ""Intrusion - but no attack - on U.S. energy grid is a warning, says former NSA official," USA Today. (September 7, 2017). Available at: https://www.usatoday.com/story/tech/news/2017/09/06/dozens-power-companies-breached-hackers-cybersecurity-researcher-says/638503001/

> In some cases, this involved access to details about how the company operated, engineering plans and equipment, in some cases even down to the level of controlling valves, pipes or conveyer belts, said Vikram Thakur, principal research manager at Symantec, which discovered the intrusions and first published information about them in a blog posting Wednesday.

An October 10, 2017 post by security firm FireEye on its website disclosed cyberattacks on U.S. electric utilities by North Korea:[15]

> We can confirm that FireEye devices detected and stopped spear phishing emails sent on Sept. 22, 2017, to U.S. electric companies by known cyber threat actors likely affiliated with the North Korean government. This activity was early-stage reconnaissance, and not necessarily indicative of an imminent, disruptive cyber attack that might take months to prepare if it went undetected (judging from past experiences with other cyber threat groups).

A February 19, 2018 article in *RTO Insider*, "Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities, "disclosed multiple teams are actively targeting U.S. electric utilities: [16]

> The cybersecurity expert whose firm discovered the malware that caused blackouts in Ukraine in 2016 told state regulators that hackers targeting the U.S. electric industry are growing more numerous and more skilled.
>
> "There are five dedicated teams targeting infrastructure sites in North America, including eight different campaigns targeting sites," Robert M. Lee, CEO of cybersecurity firm Dragos, told the National Association of Regulatory Utility Commissioners' Winter Policy Summit on Feb. 11. "This is an extreme uptick."

Common factors in media reports of cybersecurity compromise are use of malicious code, or "malware," harvesting of credentials, and reconnaissance—instead of disruption of electric grid operations. It is rare to hear reports of insertion of malware into generation equipment, substations, or control rooms; instead malware insertions are commonly into the business systems of utilities. It is notable that none of the above described incidents would definitively be "Reportable Cyber Security Incidents" under utility interpretations of the definition in the NERC Glossary: "Cyber Security Incident that has compromised or disrupted one or more

---

[15] FireEye. "North Korean Actors Spear Phish U.S. Electric Companies." Website post. (October 10, 2017). Available at: https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html

[16] Heidorn, Rich. "Expert Sees 'Extreme Uptick' in Cyber Attacks on Utilities," *RTO Insider*. (February 19, 2018). Available at: https://www.rtoinsider.com/naruc-dragos-cybersecurity-scada-86882/

reliability tasks of a functional entity." Of the media accounts above, only the *USA Today* article describes malware that might have infected operational systems and therefore would be clearly reportable under the threshold proposed in the current NOPR.

Malware Often Does Not Fall Within Reporting Thresholds

We urge the Commission to recognize that reporting of malware infection is not necessarily within thresholds set on other criteria, such as "compromise," "breach," "impact," or "disruption." The experience of another government body in setting a threshold for cybersecurity incident reporting is instructive. The European Union Agency for Network and Information Security (ENISA) implemented a "Technical Guideline on Incident Reporting"[17] in 2011 and has published annual reports since 2012. EU provisions state that Member States (MS) shall ensure that electronic communication providers will "notify the competent national regulatory authority of a *breach of security* or loss of integrity that has had a *significant impact* on the operation of networks or services." (Emphasis added.) The European incident reporting threshold is an analog to the "disruption to reliable bulk electric system operation" threshold in the current NERC reporting standard.

In its "Annual Incident Reports 2016," ENISA concluded "that malicious actions (especially cyber-attacks) are not necessarily focused on creating disruptions."[18]

> **Analysis of arising cybersecurity trends/issues**
>
> For the reporting years 2012-2016, annual reports included in total 614 incident reports with 425 incident reports (69% of total incident reports) coming from system failures. On the other side, only 34 incident reports (5,5% of total incident reports) are a result of malicious actions. Approximately 76,5% of the malicious actions consist of cybersecurity attacks, namely Denial of Service attacks, malware / viruses and network hijacks, while the rest concern deliberate damages to physical infrastructure. During all the reporting years only 3 reported incidents were caused by malware. The proportion of malicious actions (especially cybersecurity related incidents) among the total number of incidents

[17] European Union Agency For Network And Information Security. "Technical Guideline on Incident Reporting; Technical guidance on the incident reporting in Article 13a." Guideline. (Version 2.1, October 2014). Available at: https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting

[18] European Union Agency For Network And Information Security. "Annual Incident Reports 2016; Analysis of Article 13a annual incident reports in the telecom sector" Report. (June 2017). Available at: https://www.enisa.europa.eu/publications/annual-incident-reports-2016

> reported remains low due to the focus of the current regulation on the "availability" of services and networks, meaning *mostly disruptions*.
>
> *Considering the above we may conclude that malicious actions (especially cyber-attacks) are not necessarily focused on creating disruptions in Telecom*, a conclusion that has already been presented in previous versions of this report. But, what we also can conclude is that, under the current form of Art. 13a within the Electronic Telecommunication Framework Directive, we do not have a very good overview of the cyber-attacks affecting the telecommunication infrastructure in EU. Although the present incident reporting scheme currently does not allow us to see the whole picture, external sources (public reports, statistics, online articles etc.) on Telecom incidents confirm an increasing trend as regards cyber-attacks. According to PwC's Global State of Information Security, 2016 18, IT security incidents in the telecom sector increased 45% in 2015 compared to the year before.
>
> However, for the first time in the six year analysis of annual incident reports we see *malware as the detailed cause*, with the most impact in terms of average duration and user hours lost. (Emphasis added)

We learn from European experience that very few malware incidents are reported, but when malware is the cause of a disruption, it has the most impact.

We importantly observe that malware infection will likewise not necessarily fall within the proposed threshold set forth in the NOPR: "mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS."[19] We urge FERC to set a reporting threshold that includes required reporting of all malware infections, both inside and outside Electronic Security Perimeters. The best threshold for reporting of malware is simple: detection of malware wherever it is found. This is especially important because much malware is of the "Trojan Horse" or Advanced Persistent Threat (APT) varieties that are purposely inserted to lie dormant until triggered at a later date when effects will be most catastrophic—for example, during a major hurricane, or a severe solar geomagnetic storm, or prior to a combined-arms military action.

[19] NOPR at 19.

Responses to FERC Comment Prompts

Other responses for comments sought by FERC are below, organized by prompt in bold.

In sum, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop modifications to the CIP Reliability Standards described above to improve the reporting of Cyber Security Incidents, including incidents that did not cause any harm but could facilitate subsequent efforts to harm the reliable operation of the bulk electric system. The Commission seeks comment on this proposal.

As we explain elsewhere in this comment, the modifications proposed to improve the reporting of cybersecurity Incidents are unlikely to have any significant positive effect. The number of reported incidents is likely to remain minimal. Unless the NOPR is substantially revamped, much of the time and effort expended on standard-setting and rulemaking could be unproductive.

The Commission proposes to direct that NERC modify the CIP Reliability Standards to specify the required content in a Cyber Security Incident report. We propose that the minimum set of attributes to be reported should include: (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident…The Commission seeks comment on this proposal and, more generally, the appropriate content for Cyber Security Incident reporting to improve awareness of existing and future cyber security threats and potential vulnerabilities.

In developing the required content in a cybersecurity incident report, we respectfully suggest that the Commission leverage work already done by the federal government. US-CERT has

published "Federal Incident Notification Guidelines" with the following information elements required when notifying US-CERT of an incident:[20]

1. Identify the current level of impact on agency functions or services (Functional Impact).
2. Identify the type of information lost, compromised, or corrupted (Information Impact.)
3. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
4. Identify when the activity was first detected.
5. Identify the number of systems, records, and users impacted.
6. Identify the network location of the observed activity.
7. Identify the point of contact for additional follow-up.
8. Submit the notification to US-CERT.

The following information should also be included if known at the time of submission:

9. Identify the attack vector that led to the incident.
10. Provide any indicators of compromise, including signatures or detection measures developed in relation to the incident.
11. Provide any mitigation activities undertaken in response to the incident.

At present time, only two of the Commission's proposed minimum set of reportable attributes overlap with the US-CERT elements:

> (1) the functional impact, when identifiable, that the Cyber Security Incident achieved or attempted to achieve;
>
> (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident.

We propose that Commission attribute No. 3, "the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident," be added to the US-CERT list.

[20] United States Computer Emergency Readiness Team (US-CERT). "US-CERT Federal Incident Notification Guidelines." Guidelines. (Effective April 1, 2017). Available at: https://www.us-cert.gov/incident-notification-guidelines

The Commission should recognize that when malware is the attack vector, utilities have a perverse incentive to delay mitigation of the malware, because mitigation may necessitate shutdown of operational systems, causing increased costs or lost revenues, especially for merchant generators and transmission companies. A January 8, 2018 article in *EnergyWire*, "Gadfly advocates win a round on cyberattack rules," confirms this issue:[21]

> Asked whether utilities would be likely to remove malware on their own, without a specific requirement to do so, Miller said, "I've been to too many generation plants that still have Conficker running around in them," referring to a 9-year-old virus that attacks Microsoft operating systems. "If it's not impacting operations, they don't care, because the effort to take the systems offline to remove [the malware] is an outage, downtime, impact.

Accordingly, Resilient Societies proposes that an improved cybersecurity reporting standard require a second reporting attribute over and above the US-CERT attributes: "a schedule and expected completion date for additional mitigation activities."

In addition, the Commission seeks comment on whether to exclude EACMS from any Commission directive and, instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold.

Excluding Electronic Access Control or Monitoring Systems (EACMS) from the Commission directive could exempt reporting of attempted compromises. Clearly, breach of a firewall (one of the most common types of EACMS) is a serious cybersecurity incident that should be reportable.

The Commission also seeks comment on potential alternatives to modifying the mandatory reporting requirements in the NERC Reliability Standards. Specifically, we seek comment on whether a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure would effectively address the reporting gap and current lack of awareness of cyber-related incidents, discussed above, among NERC, responsible entities and the Commission, and satisfy the goals of the proposed directive.

---

[21] Behr, Peter and Sobczak, Blake. "Gadfly advocates win a round on cyberattack rules," *EnergyWire*. (January 8, 2018). Available at: https://www.eenews.net/stories/1060070313

Examination of NERC Rules of Procedure Section 1600 shows the intent of rule is to facilitate one-time requests for data. Section 1602.1, Procedure for Authorizing a NERC Request for Data or Information, reads:

> A proposed request for data or information shall contain, at a minimum, the following information: (i) a description of the data or information to be requested, how the data or information will be used, and how the availability of the data or information is necessary for NERC to meet its obligations under applicable laws and agreements; (ii) a description of how the data or information will be collected and validated; (iii) a description of the entities (by functional class and jurisdiction) that will be required to provide the data or information ("reporting entities"); (iv) the schedule or due date for the data or information; (v) a description of any restrictions on disseminating the data or information (e.g., "confidential," "critical energy infrastructure information," "aggregating" or "identity masking"); and (vi) an estimate of the relative burden imposed on the reporting entities to accommodate the data or information request.

Notably, Subsection (iv) specifies "the schedule or due date for the data or information"—"schedule" and "due date" are clearly singular nouns. This existing NERC procedure would be a poor fit for a standing order for data on cybersecurity incidents that occur continually.

The Commission seeks comment on the appropriate timing for Cyber Security Incident reporting to better ensure timely sharing of information and thereby enhance situational awareness. In addition, the Commission seeks comment on the proposal to direct NERC to file an annual report with the Commission.

In an ideal world, reporting of cybersecurity incidents would take place at machine-speed, within seconds, or even microseconds, of the incident taking place. We suggest that the Commission word its final order, including the list of reportable attributes, to allow and preferably to require automated reporting, at least for an initial report.[22] Subsequent and more complete reports, in the timeframe of several days, may require human intervention. Also, the definition of "incident" should be expanded to explicitly include detected Trojan Horse infections and Advanced Persistent Threat (APT) malware.

[22] The Department of Commerce National Institute of Standards and Technology (NIST) has developed standards for automated cyber incident reporting, including automated "vulnerability scanning." See for example, David A. Waltermire, *et al.*, *The Technical Specification for Security Content Automation Protocol (SCAP): SCAP Version 1.3,* NIST Report SP-800-126, February 14, 2018, including Section 5.2 on "vulnerability scanning" at pp. 43-44.

We especially commend for Commission's consideration the assessments and recommendations for "pilot programs" to include automated near-real-time reporting of cyber incidents impacting both the electric utility and the financial industry. Such a program for the U.S. electric utility industry is favorably considered in the August 2017 Report to the President by the National Infrastructure Advisory Council, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.[23] The NIAC Report (at page 3) endorses a pilot program for "machine-to-machine information share technologies, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed."[24]

The potential for automated cyber incident reporting opens parallel potential for automated or automated-plus-human assessment reporting at network or near-network speeds.

When new cyberattack campaigns can develop in hours or days or weeks, an annual summary report to the Commission would not be in the public interest. We suggest quarterly, or even monthly, reports from NERC to the Commission.

Moreover, FERC may seek additional voluntary reports from other recipients of cyber incident information sharing, including the industry-sponsored E-ISAC managed by NERC; and components of the U.S. Department of Homeland Security: US-CERT, ICS-CERT, and the National Cybersecurity and Communications Integration Center (NCCIC).

We encourage the FERC Commissioners to issue a Policy Paper emphasizing the primary goal of cyber incident reporting and mitigation is to attain early warning, situational awareness, and protection of the reliable operation and prompt recovery of the bulk power system from cyber incidents, whether or not malicious in origin or intent.

---

[23] National Infrastructure Advisory Council. "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report." Report. (September 1, 2017). Available at: https://www.dhs.gov/sites/default/files/publications/transmittal-letter-potus-niac-securing-cyber-assets-508.pdf

[24] The August 2017 NIAC Report further proposes: "Threat information and mitigation must move at network speed. Advances in machine-to-machine information sharing and automated mitigations show great promise." *Ibid.*, at p. 8.

Registered entities that report cyber incidents promptly and in good faith should be shielded from liability and fines. The Critical Infrastructure Protection (CIP) standards now in effect are insufficiently protective and may be unintended barriers to the network-based information sharing needs of the future.

Request for Technical Conference Held in Public Session

Too often in the past, rulemakings for reliability standards appear to have facilitated closed negotiations between FERC and NERC, with other public stakeholders denied both information and effective participation. In regard to the current rulemaking, cybersecurity vendors such as Symantec, Dragos, FireEye, and Cylance have knowledge of campaigns against U.S. electric utilities as well as critical infrastructures abroad. We respectfully request that the Commission hold a technical conference in public session, with cybersecurity firms as panelists, to obtain a more accurate picture of cybersecurity risk—especially risk from malware—and opportunities for network speed automated protections, before making a final ruling.

It is our belief that the vast majority of malware signatures currently in possession of ICS-CERT and US-CERT were reported not by electric utilities directly, but through the systems of cybersecurity vendors. Questioning of staff at ICS-CERT and US-CERT in public session could confirm that voluntary reporting of malware signatures by electric utilities directly would provide opportunities for significantly improved “best practices,” even before an enhanced reliability standard is implemented.

Finally, testimony in a public technical conference could bring forth a better threshold for cybersecurity incident reporting—a threshold that does not solely depend on compromise of Electronic Security Perimeters or Electronic Access Control or Monitoring Systems.

Supporting Recommendations of Applied Control Solutions

Resilient Societies also endorses the recommendations submitted in this Docket by a national expert on control systems, Joseph Weiss of Applied Control Solutions, LLC:

1. Require utility personnel to identify all electronic communication impacts that could affect grid reliability as being cyber-related, whether malicious or unintentional.
2. Require utilities not NERC, to disclose to FERC, ICS-CERT, the National Cybersecurity and Communications Integration Center (NCCIC), and the utility industry all control system cyber incidents in plant, transmission, distribution, or SCADA operations in an expeditious manner. This is because many cyber-related events are not unique to just one utility or facility.
3. Require training by plant and substation staff to better understand control system cyber security and to recognize upset conditions that could be cyber-related.
4. Require utility IT and physical Security Operations Centers (SOCs) to coordinate with plant and substation Operations Centers to better coordinate what upset conditions may be cyber-related."

Reliability Standard to Be Set By a Necessary Deadline

NERC has a procedure to allow an urgently needed reliability standard to be set by a necessary regulatory deadline:[25]

> **Section 16.0: Waiver**
>
> While it is NERC's intent to use its ANSI-accredited Reliability Standards development process for developing its Reliability Standards, NERC may need to develop a new or modified Reliability Standard, definition, Variance, or implementation plan under specific time constraints (such as to meet a time constrained regulatory directive) or to meet an urgent reliability issue such that there isn't sufficient time to follow all the steps in the normal Reliability Standards development process.
>
> The Standards Committee may waive any of the provisions contained in this manual for good cause shown, but limited to the following circumstances:
>
> - In response to a national emergency declared by the United States or Canadian government that involves the reliability of the Bulk Electric System or cyber attack on the Bulk Electric System;
> - Where necessary to meet regulatory deadlines;

[25] NERC. "Standard Processes Manual, VERSION 3." Effective: June 26, 2013. Available at: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Given several years of data that remains unreported under the current cybersecurity incident reporting standard, and given the national security situation where the U.S. electric grid lacks effective cyber defenses (according to the Defense Science Board's Cybersecurity Task Force), we respectfully request that FERC set a regulatory deadline for an improved Cyber Security Incident Reporting Reliability Standard.

Conclusion

The current NERC cybersecurity reporting standard fails to protect the public from catastrophic grid outages, with zero reportable cybersecurity incidents in multiple years. Even NERC admits that the "mandatory reporting process does not create an accurate picture of cyber security risk…"[26] Official government reports and disclosures by cybersecurity vendors show that multiple cyberattack campaigns are threatening the U.S. electric grid; these campaigns often include malware infections.

Malware commonly infects business systems, but infections are much less common in the operational systems of utilities—those systems behind Electronic Security Perimeters and Electronic Access Control or Monitoring Systems. Compromise of an operational perimeter is a deficient threshold for cybersecurity incident reporting, especially reporting of potential or actual malware infection. Most attackers are smart enough to not breach perimeters until the time of a full-scale attack. The best threshold for reporting of malware is simple: detection of malware wherever it is found. Moreover, cyber incidents, including impacts or attempted impacts upon control systems, whether malicious or not, should be within a class of required cyber incident reporting, preferably at network speeds.

Opportunities for automated reporting and automated protection initiatives are in the public interest. The Commission has the authority to augment the identification and reporting of cyber incidents under Section 215 of the Energy Policy Act of 2005. The Commission needs to embrace protective technologies and apply them without discrimination to all registered entities.

[26] NERC, "2017 State of Reliability Report." (June 2017), p. 4. Available at: .http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MAS TER_20170613.pdf.

The Commission should take notice of multi-year NIST and US-CERT initiatives to develop attributes for reporting characteristics of cybersecurity incidents. The US-CERT attributes are a good starting point for an improved cyber incident reporting reliability standard. Moreover, the Commission has an opportunity now to encourage and accelerate machine-to-machine pilot reporting programs for automated protections of a 21st century electric grid.

We respectfully request that FERC establish new transparency in rulemaking and standard-setting by holding a public technical conference to take testimony from cybersecurity vendors; their experts have broad and direct knowledge of cybersecurity risks, beyond knowledge of any single utility or trade association. We also urge the Commission to invite the National Infrastructure Advisory Council Task Force on Cyber Asset Protection to share their insights on opportunities for automated monitoring, scanning, and reporting, and automated defenses for cyber assets. Based on expert testimony and public comments in this rulemaking, the modifications proposed in the NOPR could be substantially revamped.

With this standard setting, FERC has the opportunity to improve the reliability standard-setting and approval process, acting not in the narrow economic interest of regulated utilities, but in the public interest.

Respectfully submitted by:

Thomas S. Popik, Chairman
thomasp@resilientsocieties.org

William R. Harris, Secretary,
williamh@resilientsocieties.org

Foundation for Resilient Societies
52 Technology Way
Nashua, NH 03060-3245
www.resilientsocieties.org

Appendix 1: Letter to NERC Board of Trustees

Foundation for Resilient Societies
52 Technology Way
Nashua NH 03060
www.resilientsocieties.org

May 12, 2016

Frederick W. Gorbet, Chair
Roy Thilly, Vice Chair
Gerald W. Cauley, President and CEO
Paul F. Barber
Janice B. Case
Robert G. Clarke
Kenneth W. DeFontes, Jr.
David Goulding
George Hawkins
Kenneth G. Peterson
Jan Schori
Board of Trustees
North American Electric Reliability Corporation
3353 Peachtree Road, N.E. Suite 600, North Tower
Atlanta, GA 30326

Dear Trustees:

We are writing in regard to your Board's pending review of the North American Electric Reliability Corporation (NERC) *State of Reliability 2016* report, scheduled for approval at the May 13, 2016 Board meeting. We are concerned this report may present misleading statistics on reportable cybersecurity incidents for the Bulk Power System during calendar year 2015.

Government policymakers and the public increasingly recognize the threat of cyberattack on critical infrastructure such as the electric grid. In December 2015, a sophisticated cyberattack took down portions of the Ukrainian electric grid. An April 2016 poll by the Pew Research Center indicates 72% of Americans view cyberattacks from other countries as a "major threat." An October 16, 2015 article published by CNN, titled "ISIS is attacking the U.S. energy grid (and failing)," disclosed that the Islamic State seeks to hack American electrical power systems.

NERC staff told us the draft *State of Reliability 2016* report has been supplied to your Board of Trustees. Section 4 of the NERC By-Laws clearly states that material provided to the Board must be publicly posted within 24 hours: "all nonconfidential material provided to the board, shall be posted on the Corporation's Web site, and notice of meetings of the board shall be sent electronically to members of the Corporation, within 24 hours of the time that notice or such material is given to the trustees." Moreover, Section 215 of the Federal Power Act mandates that NERC, as the Electric Reliability Organization (ERO), must "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards and otherwise exercising its duties."

NERC's legal staff has refused to make available the *State of Reliability 2016* report, maintaining it is "confidential." NERC's ongoing practice of restricting access to Board-provided materials—even for several days after the material is approved by the Board for public distribution and therefore cannot be "confidential"—appears to be a clear violation of NERC's own By-Laws, as well as federal law.

Conversely, were NERC to make the *State of Reliability 2016* report publicly available via the NERC website within 24 hours of submittal to the Board, stakeholders would have an opportunity to identify biases or omissions, helping the Board to improve the accuracy and utility of reliability metrics. We ask you to release the *State of Reliability 2016* report immediately. If the NERC *State of Reliability 2016* report follows the pattern of last year's report, it may contain materially misleading statements in regard to the number of reportable cybersecurity incidents. In the *State of Reliability 2015* report, NERC represented that only three (3) reportable cybersecurity incidents had occurred for the Bulk Power System in all of 2014. Our understanding is that the number of reportable cybersecurity incidents for 2015 may likewise be a very low number.

In contrast, in Fiscal Year 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security received 79 reported cybersecurity incidents from the Energy Sector. In Fiscal Year 2015, ICS-CERT received 46 reported cybersecurity incidents from the Energy Sector. It is improbable that electric utilities are immune from cybersecurity incidents that affect the Energy Sector generally. We also note that Admiral Michael Rogers, Director, National Security Agency and Commander of U.S. Cyber Command, testified to Congress on November 20, 2014 that multiple foreign nations can take down the U.S. grid—this statement is inconsistent with trivial numbers of cybersecurity incidents reported to NERC by electric utilities.

At the January 28, 2016 FERC Technical Conference on Supply Chain Risk Management, a cybersecurity expert testified that "BlackEnergy" malware is pervasive within the North American electric grid. This is the same family of malware used to acquire credentials to black out the western Ukrainian electric grid.

According to NERC Critical Infrastructure Protection standards and Glossary of Terms, a Reportable Cyber Security Incident is "A Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." When malware is detected in operational system of an electric utility, clearly a "compromise" has occurred. Malware infection may require a switch to manual operations to ensure security. Additionally, shutdown or isolation of systems may be required to remove malware. Therefore, detected malware infection should be a clear case of a "Reportable Cyber Security Incident." If NERC has a pattern and practice of permitting regulated entities to opt out of reporting malware infections and other cybersecurity incidents, this could lead to misleading statistics in the *State of Reliability* reports.

When misleading statistics are given to government policymakers, this can forestall remedial legislation and federal rulemaking necessary to protect critical infrastructures and public safety. Before approving the *State of Reliability 2016* report, we respectfully request that the NERC Board of Trustees determine if incomplete cybersecurity incident reporting by electric utilities has obscured the true risk of cyberattack on the North American electric grid.

Sincerely,

Thomas S. Popik
Chairman, Foundation for Resilient Societies