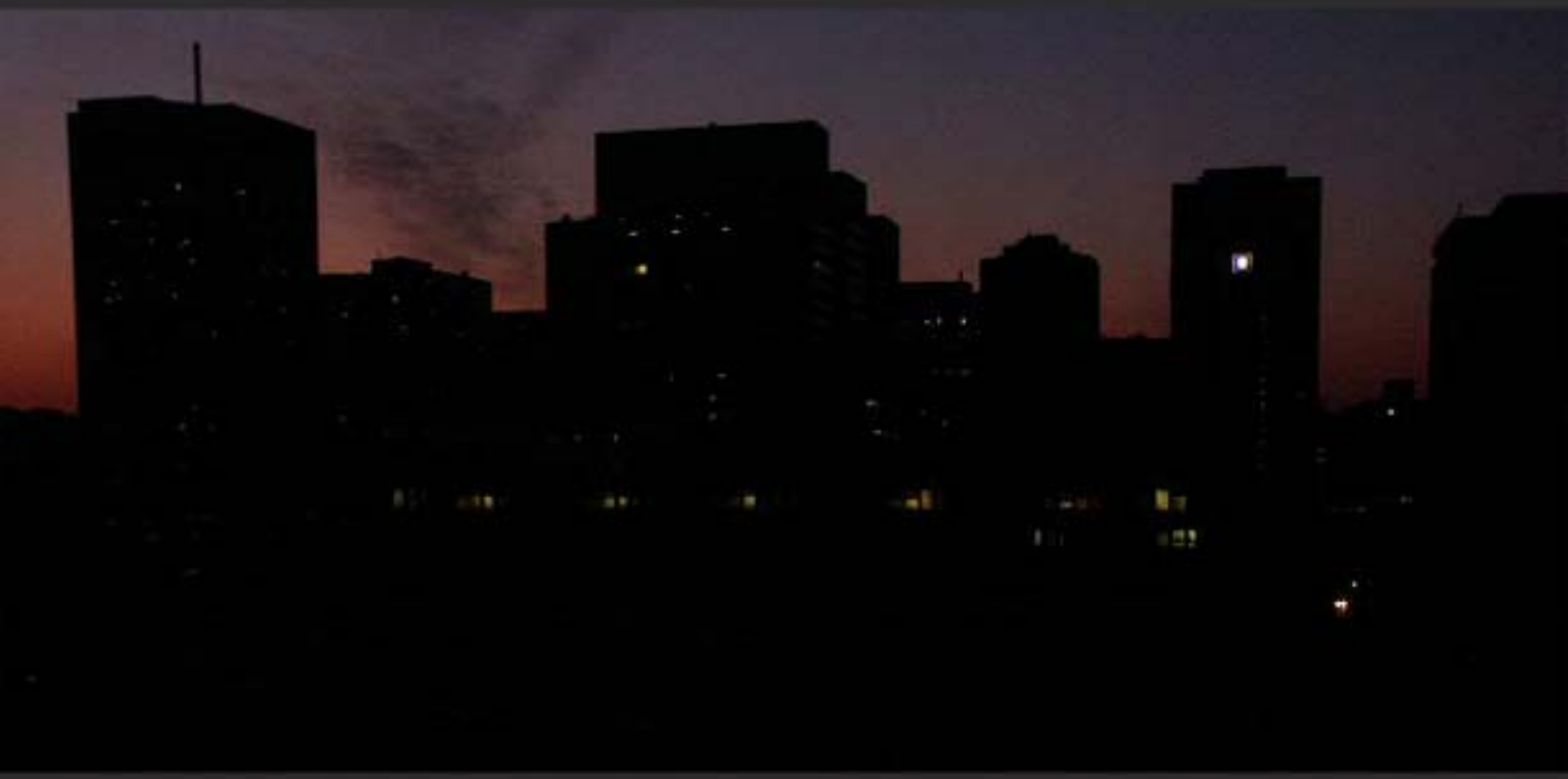
ELECTRIC GRID VULNERABILITY

Industry Responses Reveal Security Gaps



A report written by the staff of Congressmen Edward J. Markey (D-MA) and Henry A. Waxman (D-CA)

May 21, 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The last few years have seen the threat of a crippling cyber-attack against the U.S. electric grid increase significantly. Secretary of Defense Leon Panetta identified a "cyber-attack perpetrated by nation states or extremist groups" as capable of being "as destructive as the terrorist attack on 9/11."[1] A five-year old National Academy of Sciences report declassified and released in November 2012 found that physical damage by terrorists to large transformers could disrupt power to large regions of the country and could take months to repair, and that "such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction."[2] On May 16, 2013, the Department of Homeland Security testified that in 2012, it had processed 68% more cyber-incidents involving Federal agencies, critical infrastructure, and other select industrial entities than in 2011.[3] It also recently warned industry of a heightened risk of cyber-attack, and reportedly noted increased cyber-activity that seemed to be based in the Middle East, including Iran.[4]

Current efforts to protect the nation's electric grid from cyber-attack are comprised of voluntary actions recommended by the North American Electric Reliability Corporation (NERC), an industry organization, combined with mandatory reliability standards that are developed through NERC's protracted, consensus-based process. Additionally, an electric utility or grid-related entity may take action on its own initiative.

In light of the increasing threat of cyber-attack, numerous security experts have called on Congress to provide a federal entity with the necessary authority to ensure that the grid is protected from potential cyber-attacks and geomagnetic storms. Despite these calls for action, Congress has not provided any governmental entity with that necessary authority. In 2010, bipartisan cyber-security legislation known as the GRID Act passed the House of Representatives by voice vote. If enacted, this legislation would have provided the Federal Energy Regulatory Commission (FERC) with the authority to require necessary actions to protect the grid. However, this legislation did not pass the Senate and has not been taken up again by the House since that time.

To inform congressional consideration of this issue, Representatives Edward J. Markey and Henry A. Waxman requested information in January 2013 from more than 150 investor-owned utilities (IOUs), municipally-owned utilities, rural electric cooperatives, and federal entities that own major pieces of the bulk power system. As of early May, more than 60% of the entities had responded (54 investor-owned utilities, 47 municipally-owned utilities and rural electric cooperatives, and 12 federal entities). This report is based upon those responses, and finds the following:

---

[1] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
[2] http://www.nap.edu/catalog.php?record_id=12050#toc
[3] http://www.dhs.gov/news/2013/05/16/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-hearing
[4] http://articles.washingtonpost.com/2013-05-09/world/39139314_1_senior-u-s-oil-and-gas-companies-iran

1. **The electric grid is the target of numerous and daily cyber-attacks.**

    - More than a dozen utilities reported "daily," "constant," or "frequent" attempted cyber-attacks ranging from phishing to malware infection to unfriendly probes. One utility reported that it was the target of approximately 10,000 attempted cyber-attacks each month.
    - More than one public power provider reported being under a "constant state of 'attack' from malware and entities seeking to gain access to internal systems."
    - A Northeastern power provider said that it was "under constant cyber attack from cyber criminals including malware and the general threat from the Internet…"
    - A Midwestern power provider said that it was "subject to ongoing malicious cyber and physical activity. For example, we see probes on our network to look for vulnerabilities in our systems and applications on a daily basis. Much of this activity is automated and dynamic in nature – able to adapt to what is discovered during its probing process."

2. **Most utilities only comply with mandatory cyber-security standards, and have not implemented voluntary NERC recommendations.**

    - Almost all utilities cited compliance with *mandatory* NERC standards. Of those that responded to a question of how many voluntary cyber-security measures recommended by NERC had been implemented, most indicated that they had not implemented any of these measures.
    - For example, NERC has established both mandatory standards and voluntary measures to protect against the computer worm known as Stuxnet. Of those that responded, 91% of IOUs, 83% of municipally- or cooperatively-owned utilities, and 80% of federal entities that own major pieces of the bulk power system reported compliance with the Stuxnet mandatory standards. By contrast, of those that responded to a separate question regarding compliance with voluntary Stuxnet measures, only 21% of IOUs, 44% of municipally- or cooperatively-owned utilities, and 62.5% of federal entities reported compliance.

3. **Most utilities have not taken concrete steps to reduce the vulnerability of the grid to geomagnetic storms and it is unclear whether the number of available spare transformers is adequate**

    - Only 12 of 36 (33%) responding IOUs, 5 of 25 (20%) responding municipally- or cooperatively-owned utilities, and 2 of 8 (25%) responding federal entities stated that they have taken specific mitigation measures to protect against or respond to geomagnetic storms.
    - Most utilities do not own spare transformers. Only twenty IOUs, six municipally- or cooperatively-owned utilities, and eight federal entities reported owning spare transformers. While other utilities reported participation in various mutual assistance agreements or industry equipment sharing programs, none knew how many other utilities would claim contractual access to the same equipment in the event of a large-scale outage.

INTRODUCTION

The Importance of the Electric Grid

The U.S. bulk-power system serves more than 300 million people and is made up of more than 200,000 miles of transmission lines, and more than 1 million megawatts of generating capacity, and is valued at over $1 trillion. The vast majority of grid assets are owned and operated by private companies and other non-federal institutions. The components of the grid are highly interdependent and, as history has shown, a line outage or system failure in one area can lead to cascading outages in other areas. For example, on August 14, 2003, four sagging high-voltage power lines in northern Ohio brushed into trees and shut off. Compounded by a computer system error, this shut-down caused a cascade of failures that eventually left 50 million people without power for two days across the United States and Canada. This event, the largest blackout in North American history, cost an estimated $6 billion and contributed to at least 11 deaths.[5]

These vulnerabilities pose substantial risks to U.S. national security. A 2008 report by the Defense Science Board's Task Force on Department of Defense (DOD) Energy Strategy concluded that "critical missions . . . are almost entirely dependent on the national transmission grid. About 85% of the energy infrastructure upon which DOD depends is commercially owned, and 99% of the electric energy DOD installations consume originates outside the fence. . . . In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage."[6]An October 2009 report by the Government Accountability Office concluded that of DOD's 34 most critical global assets, 31 rely on commercially operated electricity grids for their primary source of electricity[7].

Grid vulnerabilities that lead to power disruptions have major economic ramifications as well. Power outages and power quality disturbances are estimated to cost the U.S. economy between $119 to $188 billion per year.[8] Single events can cost $10 billion or more.[9]

The Cyber Threat

Grid operations and control systems are increasingly automated, incorporate two-way communications, and are connected to the Internet or other computer networks. While these improvements have allowed for critical modernization of the grid, this increased interconnectivity has made the grid more vulnerable to remote cyber attacks.

Public reports relating to cyber vulnerabilities, threats, and attacks on the electric grid have increased in recent years (see the timeline in Appendix B). The first major documented vulnerability was "Aurora." In 2006, the Department of Homeland Security's Control Systems

---

[5] http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later
[6] Department of Defense, Report of the Defense Science Board Task Force on DoD Energy Strategy, More Fight—Less Fuel, at 18 (Feb. 2008).
[7] http://transition.fcc.gov/pshs/docs/clearinghouse/GAO_Defense_Critical_Infrastructure_102009.pdf
[8] http://certs.lbl.gov/pdf/55718.pdf
[9] http://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf

Security Program conducted an analysis—performed by the Department of Energy's Idaho National Laboratory—that demonstrated an attacker could hack into the control system of an electric generator or other rotating equipment connected to the grid and throw the equipment out of phase, causing severe physical damage to the equipment.

Cyber-attacks can create instant effects at very low cost, and are very difficult to positively attribute back to the attacker. It has been reported that actors based in China, Russia, and Iran have conducted cyber probes of U.S. grid systems, and that cyber-attacks have been conducted against critical infrastructure in other countries. There are numerous examples of such cyber-attacks, including the attack on Saudi Aramco, which destroyed the hard drives of more than 30,000 computers at the Saudi state-run oil company.[10] According to recent reports, intrusions into ten major American energy companies were similarly attempts to disrupt or destroy administrative systems.[11] The rate of such cyber-attacks against American corporate and government infrastructure is on the rise and unlikely to abate.

There also has been growing attention to physical vulnerabilities of the grid. For example, the replacement of large transformers essential to the reliable operation of the grid may require twenty months or longer[12]. A limited number of spare, large transformers are available within the United States, and industry has developed a voluntary program (the spare transformer equipment program, or ''STEP'') providing for sharing of such assets in the event of a terrorist attack. But it is unclear whether this program would prove adequate in the event of a coordinated physical attack on one or more transformers.

A special subset of physical vulnerabilities and threats is associated with electromagnetic pulse (EMP) and geomagnetic disturbance (GMD). EMPs can be generated intentionally by utilizing portable equipment to produce high-power radio frequency or microwave or other electromagnetic pulses that destroy or disable electronic equipment. Such weapons can vary in size from a hand-held device to a large vehicle-borne device, can be used at a distance from a target, and can penetrate walls or other obstacles—making detection and attribution of an attack to a specific source difficult. More than a dozen countries have conducted research on such weapons, and DOD has demonstrated that such weapons can be developed with modest financial resources and technical capability. Such weapons have been used to defeat security systems, commit robberies, disable police communications, induce fires, and disrupt banking computers.

GMDs occur naturally through geomagnetic storms resulting from solar activity. A 2008 National Academy of Sciences report[13] estimated the effects of a geomagnetic storm of the magnitude of the 1921 storm on the current electrical grid, concluding that such a storm could cause permanent damage to more than 350 transformers, leaving as many as 130 million people without power. Impacts from a large geomagnetic storm could last for several years and cost in the range of several trillion dollars per year[14].

---

[10] http://articles.washingtonpost.com/2013-05-09/world/39139314_1_senior-u-s-oil-and-gas-companies-iran
[11] http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&_r=0
[12] http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf
[13] http://books.nap.edu/catalog.php?record_id=12507#toc
[14] http://books.nap.edu/catalog.php?record_id=12507#toc

On October 18, 2012, FERC issued a notice of proposed rulemaking (NOPR) which proposed to direct NERC to submit for approval reliability standards to address the impacts of GMDs on the bulk power system.[15] In its comments on the NOPR, NERC noted that America's bulk power system was not designed to withstand the effects of a severe solar storm. It also noted that the effects of an EMP are significantly more extensive than a GMD and urged the Commission in its final rule to clarify that issues related to EMPs are outside the scope of the final rule.[16] FERC's final rule was issued on May 16, 2013. It directs NERC to file reliability standards within eight months that require owners and operators of the bulk power system to establish operational procedures to mitigate the effects of GMDs. Additionally, within eighteen months, NERC must file reliability standards which identify "benchmark GMD events" that utilities must assess the potential impacts of. If the assessments identify effects of such events, then the standards must require utilities to protect against them. FERC's order does not direct NERC to develop reliability standards to mitigate the effects of EMPs.

Through the 2001 Floyd D. Spence National Defense Authorization Act, Congress established a commission to assess the threat of electromagnetic pulse from a high-altitude nuclear detonation, vulnerabilities of military and civilian infrastructure to such an attack, and the feasibility and cost of protecting such infrastructure. The 2004 report[17] concluded that the risks from high-altitude EMP to the U.S. electric grid are substantial and recommended that measures be taken to protect high-value transmission assets that would require a long lead time to replace, key electric generation capability, and critical communication channels.

Key government officials responsible for U.S. national security and grid reliability have put the cyber threat in stark terms and called for urgent action. In September 2011, in testimony before the House Energy and Commerce Committee, all five commissioners of the Federal Energy Regulatory Commission (FERC) agreed that the threat of a cyber-attack on the electric grid was the top threat to electricity reliability in the United States.[18] In July 2012, FBI Director Robert Mueller testified before the Senate Select Committee on Intelligence that physical terrorist attacks were the leading national security threat but that "down the road, the cyber-threat, which cuts across all [FBI] programs, will be the number one threat to the country." In October 2012, Defense Secretary Panetta warned that the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to attacks from foreign hackers who could disable the nation's grid and other critical infrastructure.[19]

---

[15] http://www.ferc.gov/whats-new/comm-meet/2012/101812/E-2.pdf
[16] http://www.balch.com/files/upload/NERC%20Comments%20on%20GMD%20NOPR_FINAL.pdf
[17] http://www.empcommission.org/docs/empc_exec_rpt.pdf
[18] http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/091411%20EP%20The%20American%20Energy%20Intiative%2012%20-%20Impacts%20of%20the%20Environmental%20Protection%20Agency%27s%20New%20and%20Proposed%20Power%20Sector%20Regulations%20on%20Electric%20Reliability.pdf
[19] http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Legislative and Regulatory Action

As part of the Energy Policy Act of 2005, Congress added a new provision to the Federal Power Act, Section 215, which provided for the establishment of mandatory reliability standards for the bulk-power system, including standards addressing cyber-security threats. Under section 215, FERC has designated the North American Electric Reliability Corporation (NERC) as the electric reliability organization responsible for proposing, for FERC review and approval, reliability standards to protect and enhance the reliability of the bulk-power system, including cyber-security standards.

NERC is a not-for-profit corporation, the principal members of which are owners and operators of the bulk-power system. More than 1,800 different entities own or operate components of the bulk-power system that is subject to the NERC standard-setting process. NERC's standards committee develops standards through an open, time-consuming process. Before reliability standards can become mandatory and enforceable, NERC's utility membership must approve them. Approval requires a quorum of 75 percent of the stakeholder ballot pool and support from a supermajority of at least two-thirds of the votes.

Under section 215, FERC cannot prescribe its own standards or directly amend NERC's standards, but it has authority to direct NERC to develop standards to address a particular vulnerability or to modify existing standards. The process of developing these reliability standards is lengthy (see Appendix B for a timeline). It can take NERC six months or longer to respond to FERC's initial order to submit reliability standards. It then takes FERC months to review these proposed standards. FERC can reject the proposed standards or request additional work if they are insufficient, adding further delays to implementation of any required measures.

For example, the first critical infrastructure protection (CIP) standards approved by FERC in January 2008 took more than three years for NERC to develop (although part of this period predated the 2005 law that authorized the development of mandatory standards). It subsequently took NERC 43 months to develop and submit the most recent Version 5 of the CIP standards to FERC for approval. Such timeframes are not well suited to address rapidly evolving grid security vulnerabilities.

While NERC has received FERC approval for procedures that allow for an accelerated process for developing standards in case of a ''national security emergency situation,'' these procedures still require a consensus approach to be taken. When NERC attempted to use these procedures to turn 25 recommended measures related to remote access to assets into a mandatory standards proposal, the measures were ultimately voted down in their entirety by industry and thus remain voluntary. Some of those recommended measures have been incorporated into the CIP Version 5 standards that may become mandatory by 2016, approximately six years after they were initially put forth as necessary to respond to an emergency national security situation. But the vast majority of those 25 recommendations are not part of the pending CIP Version 5 standards.

To date, FERC has approved nine CIP reliability standards developed by NERC, addressing critical cyber asset identification, security management controls, personnel and training, electronic security perimeters, physical security of critical cyber assets, systems security management, incident reporting and response planning, and recovery plans for critical cyber assets.

However, NERC's record with regard to taking prompt action on grid security vulnerabilities and threats has raised concerns. For example, more than six years after the identification of the Aurora vulnerability discussed above, NERC still has not proposed any reliability standard directly addressing that vulnerability. Moreover, NERC's CIP standards only apply to assets identified by utilities as critical. In a December 2008 NERC survey of self-certification of critical assets and critical cyber assets, only 31% of respondents to the survey, and only 29% of owners and operators of electric generation, identified even a single critical asset.

In order to respond to these challenges and provide FERC with authority to issue orders in response to known cyber threats and vulnerabilities to the grid, Representatives Ed Markey (D-MA) and Fred Upton (R-MI) introduced the bi-partisan GRID Act, HR5026, in the 111th Congress. The bill was reported by the Energy and Commerce Committee by a vote of 47-0 and passed the full U.S. House of Representatives by voice vote on July 6, 2010. However, the Senate did not act on the legislation.

The GRID Act is still viewed as necessary by those familiar with the limitations of the NERC standard-setting process. On May 31, 2011, Mr. Joseph McClelland, Director of FERC's Office of Reliability testified at an Energy and Commerce Committee hearing, stating:

> "In addition, although the NERC standards development process as envisioned in section 215 can be fine for routine reliability matters, it is too slow, too open and too unpredictable to ensure its responsiveness in the cases where national security is endangered. This process is inadequate when measures or actions need to be taken to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information."

Additionally, on September 14, 2011, at another hearing of the House Energy and Commerce Committee, all five FERC Commissioners told Rep. Edward J. Markey that not only was grid security at the top of their list of reliability concerns, but that they all believed that FERC needed the additional authority provided for in the GRID Act to address the cyber-threat to the grid[20].

---

20 http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/091411%20EP%20The%20American%20Energy%20Intiative%2012%20-%20Impacts%20of%20the%20Environmental%20Protection%20Agency%27s%20New%20and%20Proposed%20Power%20Sector%20Regulations%20on%20Electric%20Reliability.pdf

On February 12, 2013, President Obama signed an executive order identifying sectors that will be considered critical infrastructure, requiring improvements in government-to-private sector information sharing, requiring the creation of a voluntary Cyber-security Framework for critical infrastructure entities, and directing agencies to reevaluate and improve their regulations based on the Cyber-security Framework. However, the Executive Order can not provide agencies with additional statutory authority with which to address cyber risks. That can only be accomplished through an act of Congress.

While the cyber threat continues to grow, House Republicans who previously sponsored or voted for the bipartisan GRID Act have not supported reintroduction of the bill in either the 112th or 113th Congress.

METHODOLOGY

On January 17, 2013, Representatives Markey and Waxman sent a letter containing fifteen questions to more than 150 investor-owned utilities, municipally-owned utilities, rural electric cooperatives, and federal entities that own major pieces of the bulk power system (see Appendix A). As of early May[21], responses were received from 54 investor-owned utilities, 47 municipally-owned utilities and rural electric cooperatives, and 11 federal entities[22]. In addition, several responses were received from trade associations representing utilities and from individual utilities that did not receive the request letter.

The detail of the responses to the request letter varied widely. While some utilities provided complete and thorough responses (see Table 6 for a list of these), some utilities did not respond at all (see Table 4) and others provided responses that were incomplete or non-responsive (see Table 5).

Some entities refused to answer any specific questions – even requests for basic information such as how much electricity the entity generated in 2012 or the title of the individual principally responsible for the entity's cyber-security efforts. Others provided only a few paragraphs containing non-specific information in response to the inquiry.

A number of utilities also used identical or nearly-identical language to describe their general corporate policy regarding cyber-security, to outline their views on the need for cyber-security legislation, and to respond to specific questions posed. For example, three utilities submitted near- identical text for the majority of their responses, seven utilities used a phrase identical or nearly identical to one that described mandatory standards as a "very good foundation for a defense in depth framework and from which to respond to imminent threats," and there were twenty instances of utilities drawing from letters submitted to Reps. Markey and Waxman by the National Rural Electric Cooperative Association, the American Public Power Association, NERC or the Edison Electric Institute.

[21] The numeric portions of this analysis do not include a small number of responses that were received after April 1, 2013.

[22] The Army Corps of Engineers provided separate responses for six different regional divisions, and for purposes of this analysis these are treated as six separate federal entities.

FINDINGS

Finding 1: The electric grid is the target of numerous and daily cyber-attacks.

Respondents were asked to indicate how many attempted and successful physical and cyber-attacks on their systems had been experienced in each of the past five years, whether any damage to their systems resulted, and whether such attacks had been reported to federal or other authorities. While some utilities reported that they had experienced no attacks that adversely impacted their operations, many failed to respond to the question about the numbers of *attempted* attacks, and others failed to respond to the question at all.[23] One respondent stated that it did not begin to maintain records on these attacks until NERC directed entities to do so. However, many utility responses provided valuable insights into the nature of the cyber threat to the electric grid:

- More than a dozen utilities reported "daily," "constant," or "frequent" attempted cyber-attacks ranging from phishing to malware infection to unfriendly probes. One utility reported it was the target of approximately 10,000 attempted cyber-attacks each month.
- More than one public power provider said it was under a "constant state of 'attack' from malware and entities seeking to gain access to internal systems."
- A Midwestern power provider said it experienced probes and attacks via the Internet on a daily basis.
- A Northeastern power provider said that it was "under constant cyber attack from cyber criminals including malware and the general threat from the Internet, and like many energy organizations [it] comes under the scrutiny of activists."
- A Midwestern power provider said that it was "subject to ongoing malicious cyber and physical activity. For example, we see probes on our network to look for vulnerabilities in our systems and applications on a daily basis. Much of this activity is automated and dynamic in nature – able to adapt to what is discovered during its probing process."
- A large Southeastern power provider said that it had "experienced instances of malware, phishing, scans of our internet connections and other cyber security-related events."

No utility reported damage to any of its cyber-assets. However, there did not appear to be a uniform process for reporting attempted cyber-attacks to the authorities; most respondents indicated that they follow standard requirements for reporting attacks to state and federal authorities, did not describe the circumstances under which these requirements would be triggered, but largely indicated that the incidents they experienced did not rise to reportable levels.

Of the utilities that responded[24] to the request for information regarding attempted and successful physical attacks, most indicated that the only physical attacks experienced on their systems seemed linked to acts of vandalism and thefts of copper. Most incidents appeared unrelated to terrorism. However, one federal entity that owns a major piece of the bulk power

[23] 23 IOUs, 21 municipally- or cooperatively-owned utilities, and 3 federal entities that own major pieces of the bulk power system responded in some manner to the request for the number of attempted and successful cyber-attacks.
[24] 18 IOUs, 17 municipally- or cooperatively- owned utilities, and 6 federal entities that own major pieces of the bulk power system responded to this question.

system reported a Molotov cocktail was thrown at a dam. Another reported that during a copper theft, phone lines were cut which resulted in a loss of connectivity to some supervisory control and data acquisition systems and consequently impacted some electric generation assets. The incidents described by utilities highlight the potential for terrorists to access portions of the bulk power system for purposes of carrying out physical attacks.

Finding 2: Most utilities only comply with mandatory cyber-security standards and have not implemented voluntary NERC recommendations.

Utilities were asked several questions about the degree to which they comply with mandatory NERC cyber-security standards approved by FERC and additional voluntary cyber-security measures recommended by NERC. For example, NERC recommended twelve measures to respond to the Stuxnet threat. Five of the twelve recommended measures were included in a mandatory NERC standard, while the remaining seven measures are voluntary. Utilities were asked how many of the five mandatory standards and how many of the seven voluntary Stuxnet measures they had implemented.

Utilities were also asked whether they undertake background checks of employees. This is especially important in light of recent reports by the Department of Homeland Security and private security companies documenting numerous cyber-attacks by the Chinese government over the past few years. The attacks have targeted oil pipelines, electric grids, and other critical infrastructure. There were 198 such attacks in 2012 according to DHS, a 52% increase from 2011.[25] Additionally, DHS released an alert on May 9, 2013 warning industry and government officials of the serious threat posed by cyber-attacks. Such attacks could disrupt control processes or even wipe the hard drives of every computer on a network, as in the case of Saudi Aramco.[26]

Table 1 provides a summary of these responses, which reference mandatory standards and voluntary recommendations to address the Aurora and Stuxnet vulnerabilities, standards on personnel security assessments, and the requirement to conduct at least annual cyber-security response exercises. An analysis of the utility responses indicates:

- Almost all utilities cited compliance with *mandatory* standards imposed by FERC. Those that did not indicate compliance with all such standards usually indicated that such standards did not apply to them (for example, because they owned no assets to which the standards applied, because their systems were physically isolated from the internet and thus not vulnerable to attack, or because they complied with standards set by a different federal agency), or stated that they had taken measures to address the relevant threats but did not explicitly state that they were in compliance with mandatory standards.

- Most utilities did not indicate how many of the *voluntary* cyber-security measures related to Stuxnet, Aurora and remote access threats they have implemented. Of those that did respond, most indicated that they had not implemented any of these measures.

[25] http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html
[26] http://articles.washingtonpost.com/2013-05-09/world/39139314_1_senior-u-s-oil-and-gas-companies-iran

- For example, of those that responded to the question regarding compliance with mandatory Stuxnet standards, 91% of IOUs, 83% of municipally- or cooperatively-owned utilities, and 80% of federal entities that own major pieces of the bulk power system reported compliance. By contrast, of those that responded to a separate question regarding compliance with voluntary Stuxnet measures, only 21% of IOUs, 44% of municipally- or cooperatively-owned utilities, and 62.5% of federal entities reported compliance.

- Thirty-four out of thirty-five responding IOUs, seventeen out of twenty-seven responding municipally- or cooperatively-owned utilities, and two out of eight responding federal entities that own major pieces of the bulk power system reported that they utilize personnel screening that appears to be consistent with NERC's mandatory standards (i.e. screening at the time of employment and periodically thereafter, enhanced screening for those whose jobs require them to access critical assets, etc).

- A small number of utilities did not respond to questions related to the number of cyber-security recommendations they had implemented because they stated that they had either no record of receiving the NERC communication or did not know which referenced NERC communication the question was referring to.

Table 1: A summary of utility responses

	IOUs (# comply/# respondents)	Municipally- & Cooperatively- owned utilities (# comply/# respondents)	Federal entities (or regions) that own major pieces of the bulk power system (# comply/# respondents)
5 mandatory Stuxnet measures	41 of 45[27]	25 of 30[28]	8 of 10[29]
Most/all of 7 voluntary Stuxnet measures	4 of 19[30]	4 of 9[31]	5 of 8[32]
Most/all voluntary Aurora measures	7 of 13[33]	3 of 8[34]	5 of 5[35]
Personnel Screening – consistent with mandatory FERC standards	34 of 35[36]	17 of 27[37]	2 of 8[38]
Identification of "bright line" cyber assets[39]	16 of 31 done, 15 by deadline	15 of 27 complete, 11 by deadline	4of 8 complete, 4 by deadline
At least annual cyber-security simulations	25 of 36[40]	18 of 28[41]	1 of 11[42]

[27] One IOU stated it complies with 4 of 5 (and will implement the 5th), 1 said "most," another said it "initiated appropriate mitigation activities in a manner consistent with NERC's recommendations" and another provided a list of 7 specific measures but did not indicate how these corresponded to the mandatory standards.
[28] One did not receive the notice from NERC but worked with its power district to implement measures, one "utilized the recommendations" to "address the threat," and one said it has no critical assets and only the first 4 recommendations apply to its operations, and 2 said none of the standards applied to their assets.
[29] One entity said it had not implemented any because its cyber-assets are isolated and there is no way cyber-attacks to occur, and 1 said the measures were not required of its assets.
[30] Six IOUs said none were implemented, 7 said "some," "several" or "as applicable," and 2 provided a specific number of implemented measures.
[31] One stated it was using the recommendations to address the threat, 1 said it was going "beyond the requirements of the NERC standards" but did not indicate how many voluntary measures were implemented, 1 said none, and one said it has no critical assets to which the standards apply.
[32] Two stated they had implemented 6 of 7, 3 said they implemented none, one stated it had implemented all.
[33] The 7 noted "many", "most," "all applicable," or 22 of 27. One responded with 6 of 33, 1 implied that none were implemented and 3 said none were implemented.
[34] Two respondents indicated that some had been implemented, two said they had not implemented any measure, and one said they had no critical assets.
[35] One respondent indicated that one recommendation was not yet implemented.
[36] One respondent said they perform no personnel surety measures, 20 reference the FERC requirements, and 14 all list specific measures (such as criminal background checks for new hires and those with access to critical assets) that are consistent with FERC requirements, but do not explicitly reference them.
[37] Twelve respondents cited the FERC requirements, 5 list specific measures (such as criminal background checks for new hires and those with access to critical assets) that are consistent with FERC requirements, but do not explicitly reference them, 1 said they perform none because they have no critical assets, and 9 indicated they do some sort of personnel screening but did not specify measures.
[38] Six respondents referenced DOD requirements for background checks rather than FERC.
[39] After utilities submitted their responses to this question, this requirement was replaced by a new requirement in NERC's proposed CIP Version 5.
[40] Eight respondents said they conducted exercises but did not specify frequency, 2 indicated less than annual frequency of cyber-security exercises, and 1 said it did not conduct such exercises at all.
[41] Four did not indicate the frequency of exercises, and 6 indicated they did not conduct such exercises at all.
[42] Three did not indicate the frequency of exercises, and 6 indicated less than annual frequency.

Finding 3: Most utilities have not taken concrete steps to reduce the vulnerability of the grid to geomagnetic storms and it is unclear whether the number of available spare transformers is adequate

Geomagnetic Storms

Utilities were asked to describe steps they have taken to mitigate against the impact of geomagnetic storms. Geomagnetic disturbances occur when solar storms on the surface of the sun send electrically charged particles towards Earth, where they interact with the planetary magnetic field. These events are relatively frequent and can cause extensive damage to global power grids. In 1859, a massive geomagnetic storm wreaked havoc with telegraph lines across the United States and the world. In 1921, a similar geomagnetic storm destroyed American infrastructure. A much smaller storm that lasted only 92 seconds in 1989 disabled Quebec's power grid for nine hours[43] [44]. Electro-magnetic pulse (EMP) events result from a burst of electromagnetic radiation and can similarly damage or destroy critical infrastructure.

While many utilities were aware that FERC directed NERC to undertake a standard on geomagnetic storms[45] or were participating in government or industry efforts to assess vulnerabilities or evaluate mitigation processes or technologies, a much smaller number of utilities reported taking specific mitigation measures or monitoring their equipment to detect disturbances:

- Of the thirty-six IOUs that responded to this question, only twelve (33%) reported taking specific mitigation measures, such as hardening of equipment or implementing procedures for responding to events. Only six reported monitoring their equipment to detect disturbances. Six IOUs stated that they were not at risk of geomagnetic disturbances (based on either their geographic location or the type of equipment their systems utilize), twenty-two were monitoring or participating in efforts by NERC, FERC, EPRI, or others, nine are in the process of analyzing their specific vulnerabilities, and four referred to non-specific policies or practices.

- Of the twenty-five municipally- or cooperatively-owned utilities that responded to this question, only five (20%) reported taking specific mitigation measures. Only two reported monitoring their equipment to detect disturbances. Two reported that they were taking no steps to monitor, assess, or mitigate against the threat. Nine municipally- or cooperatively-owned utilities stated that they were not at risk of geomagnetic disturbances, seven were monitoring or participating in efforts by other organizations, two are in the process of analyzing their specific vulnerabilities, and three referred to non-specific policies or practices.

[43] http://www.nerc.com/files/1989-Quebec-Disturbance.pdf
[44] http://www.popularmechanics.com/science/space/deep/the-looming-threat-of-a-solar-superstorm-6643435
[45] http://www.ferc.gov/whats-new/comm-meet/2012/101812/E-2.pdf

- Of the eight federal entities that own major pieces of the bulk power system that responded to this question, only two (25%) reported taking specific mitigation measures. Only one reported monitoring its equipment to detect disturbances. Two federal entities stated that they were not at risk of geomagnetic disturbances, two were monitoring or participating in efforts by other organizations, and one is in the process of analyzing its specific vulnerabilities.

Access to Spare Transformers

Large transformers are essential to the reliable operation of the electric grid. Transformers are vulnerable to physical attacks and geomagnetic disturbances. Utilities were asked how many large transformers that were part of the bulk electric system their operations used, and how many spare transformers they owned or had contractual access to in the event their transformers were disabled by an attack or unintentional event.

While many utilities did not respond with the requested specific information, an examination of the responses indicate a wide range of utility preparations for an event in which one or more large transformers are rendered inoperable. Larger utilities seemed more likely than smaller ones to own spare transformers or participate in programs that pool industry resources so as to have contractual access to spares. However, no utilities indicated that they knew which other utilities might also have contractual access to the same equipment. It is unclear whether sufficient spare transformer capacity exists to maintain operations in the event of a sector-wide cyber-attack or other widespread reliability challenge. An analysis of the utility responses indicates:

- Only twenty IOUs reported owning spare transformers.
- Eleven IOUs reported that they both owned spare transformers and had contractual access to others, eight IOUs reported that they had contractual access to spare transformers but did not own their own, and five IOUs either had no access to spare transformers or did not believe they needed any (for example, because their systems were small or not connected to the bulk electric system).

- Only six municipally- or cooperatively-owned utilities reported owning spare transformers.
- Four municipally- or cooperatively-owned utilities reported that they both owned spare transformers and had contractual access to others, four municipally- or cooperatively-owned utilities reported that they had contractual access to spare transformers but did not own their own, and eight municipally- or cooperatively-owned utilities either had no access to spare transformers or did not believe they needed any.

- Eight federal entities reported owning spare transformers. No federal entity indicated that they had contractual access to other spare transformers.

.

Appendix A

Congress of the United States
Washington, DC 20515

January 17, 2013

To Whom It May Concern:

We write to request information regarding your entity's efforts to ensure that your electric grid assets are protected from a cyber or physical attack or geomagnetic storm. We ask that you provide responses to the following questions from your entity and, if applicable, separately from each of your U.S. subsidiaries that own or operate pieces of the bulk power system. We further request that you submit your response electronically if possible to each of the staff members listed below no later than Friday, February 15, 2013. If you have questions or concerns, please contact Michal Freedhoff (Rep. Markey, 202-225-2836 or michal.freedhoff@mail.house.gov) or Jeff Baran (Rep. Waxman, 202-225-4407 or jeff.baran@mail.house.gov).

Sincerely,

Edward J. Markey
Ranking Member
House Natural Resources Committee

Henry A. Waxman
Ranking Member
House Energy & Commerce Committee

Questions

1) What is the name of the entity for which these responses are being submitted and how much electricity did the entity generate in 2012?

2) In September 2010, the North American Electric Reliability Corporation (NERC) issued twelve recommendations to address vulnerabilities to the Stuxnet computer worm.
   a) Five of those recommendations were eventually included in mandatory Federal Energy Regulatory Commission (FERC) Critical Infrastructure Protection (CIP) standards. How many of these five recommendations have been fully implemented by your entity? If they have not been implemented, why not?
   b) The remaining seven recommendations are not currently mandated by any FERC CIP standard. How many of these seven recommendations have been implemented by your entity? If they have not been implemented, why not?

3) On October 13, 2010, in response to the Aurora malware threat to the grid, NERC issued i) nine recommendations and four options related to protection and control engineering practices, ii) five mitigation measures to address electronic and physical security, iii) nine examples of ways to address access control, iv) suggested actions related to monitoring and reporting, v) suggested actions on training, vi) suggested actions and three examples of means to conduct personnel risk assessments and vii) suggested action and three examples related to information protection to its members. None of these have been included or proposed to be included in a mandatory FERC CIP standard. How many of these recommendations, options and suggested actions have been fully implemented by your entity? If they have not been implemented, why not?

4) On March 31, 2010, NERC issued twenty-five recommendations to address an FBI warning it received related to the ability of cyber-intruders to remotely gain access to utility assets.
   a) Eight of those recommendations were eventually proposed for inclusion in a mandatory FERC CIP standard. How many of these eight recommendations have been fully implemented by your entity? If they have not been implemented, why not?
   b) The remaining seventeen recommendations are not currently planned for inclusion in any FERC CIP standard. How many of these seventeen recommendations have been implemented by your entity? If they have not been implemented, why not?

5) For each of the past five years, please indicate how many additional notices related to grid security containing a) Recommendations and b) Essential Actions were received by your entity from NERC. For each such notice, please indicate i) the type of notice, ii) the degree to which the notice related to grid security, iii) how many actions were included as part of

each notice, and iv) how many of these recommended actions have been fully implemented by your entity. (If any of the actions have not been implemented because they are not applicable to your entity, please also indicate this in your response.)

6) More recently, other cyber-vulnerabilities that could pose risks for the grid have emerged. These include but are not limited to vulnerabilities to computer malware including Flame, Shamoon, and Gauss. For each of these vulnerabilities, please describe what steps your entity has taken to protect the entity's assets against the vulnerability. If you have not taken any measures, why not?

7) Does your entity currently utilize security protocols, special measures or other hiring practices to assess whether current and/or prospective employees could pose an insider cyber-security threat? If so, please describe them. If not, why not?

8) Are there any functions or job duties that you do not permit foreign nationals to undertake at your entity? If so, please list these functions or job duties.

9) How many large transformers (meaning an electric transformer that is part of the bulk-power system) does your entity utilize? How many large transformers does your entity have contractual access to in the event that any of the large transformers utilized by your entity are rendered inoperable by a cyber-attack, accident or natural disaster? How many other entities could have similar competing claims to the same large transformers in the event of a wide-spread cyber-attack, accident or natural disaster?

10) In each of the past five years, please indicate whether your entity has been subjected to one or more attempted or successful physical or cyber-attack. For each year, please list a) the number of attempted physical attacks on your entity, b) the number of attempted cyber attacks on your entity, c) whether any such attack caused significant damage (and if so, please describe the nature of both the attack and the damage caused), d) how many attacks were reported to FERC, NERC, DHS, or other authority (and identify which authority in each case), and e) what measures were taken to prevent future similar attacks from taking place.

11) Please describe any steps your entity has taken to protect against the effects of geomagnetic storms.

12) For each of the past five years, please indicate a) how many individuals working for your entity had as one of their primary responsibilities efforts to protect your entity against cyber-attacks and b) the title of the individual with primary authority over your entity's cyber-security efforts.

13) Has your entity identified and documented all the critical cyber assets under its ownership or control based on the "bright line" criteria for identifying critical assets that was approved as part of the Version 4 CIP reliability standards? If not, when do you plan to complete the process of identifying and documenting critical cyber assets?

14) Do you believe that the current FERC CIP standards are adequate to protect against all known grid security vulnerabilities? Why or why not?

15) Does your organization conduct simulations of cybersecurity breaches or other exercises to assess the potential impacts of a cyber-attack on your entity's assets as well as on the adequacy of your entity's protocols for responding to such an attack? If so, please describe your simulations and indicate their frequency. If not, why not?

Appendix B: A timeline of threats to the electric grid and federal responses

Fall, 2001: The Nuclear Regulatory Commission (NRC) issued a security advisory to nuclear reactors to enhance cyber security in the wake of the 9/11 attacks.

April, 2003: NRC issued a security order[46] defining the design basis threat (DBT) that its licensees would be required to protect against, and this included a cyber-security component.

May 2003: NERC started to develop Version 1 of the Critical Infrastructure Protection (CIP) Standards. It took more than 40 months to submit these to FERC.

August 8, 2005: The Energy Policy Act was enacted, and included Rep. Markey's provision to require the inclusion of cyber-security consideration in the NRC's regulations for securing nuclear reactors.

August 28, 2006: NERC submitted Version 1 of its CIP Standards to FERC for approval.

December 11, 2006: FERC requested additional information from NERC on its Version 1 CIP standards proposal.

January 2007: NRC finalized its post-9/11 DBT for nuclear reactor security, incorporating requirements from the 2005 Energy Policy Act. The DBT included a cyber-security component.

February 12, 2007: NERC submitted additional information to FERC on its Version 1 CIP standards proposal.

March, 2007: The first experiments and research on the Aurora vulnerability were conducted by the Department of Energy[47] and showed how hacking into a power plant's control system could cause a generator to self-destruct.

July 20, 2007: FERC issued its Notice of Proposed Rulemaking to approve the Version 1 CIP standards.

Fall, 2007: A report entitled *Terrorism and the Electric Power Delivery System*[48] was assembled by the National Academies of Science. The report found that a widespread attack on the American electric grid could be extremely damaging and would pose little risk to the attackers. The report found that an attack could cause more damage to the system than natural disasters, black out large regions of the country for weeks or

[46] http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-053.html
[47] http://www.cnn.com/2007/US/09/26/power.at.risk/
[48] http://www.nap.edu/catalog.php?record_id=12050#toc

months, and cost billions of dollars. The Department of Homeland Security classified the report and prevented its release for five years, until November 2012.

January 18, 2008: FERC approved final Version 1 CIP standards.

March 2009: NRC issued a new rule entitled "Protection of Digital Computer and Communication Systems and Networks," which required licensees to submit a new cyber security plan and an implementation timeline for NRC approval. NERC also started to develop its Version 2 CIP Standards.

April 10, 2009: Secretary of Homeland Security Janet Napolitano acknowledged publicly[49] that the electric grid was hacked and is vulnerable to cyber-attacks.

April 21, 2009: NERC issued an alert[50] regarding the conficker worm, a type of virus that targets Microsoft Windows operating systems and was first discovered in 2008. The worm has proven very difficult to eradicate, as it is known to hide in numerous places on host machines, and has the ability to regenerate itself.

April 29, 2009: Representatives Barrow, Waxman, and Markey introduced the Bulk Power System Protection Act of 2009, to amend the Federal Power Act to give FERC authority to issue emergency orders to protect the electric grid from a range of natural, physical, and cyber threats.

May 22, 2009: NERC submitted Version 2 of its CIP Standards to FERC for approval.

July 2009: NERC started to develop its Version 5 CIP standards.

September 30, 2009: FERC approved final Version 2 CIP standards.

October 2009: NERC started to develop its Version 3 CIP Standards.

December 29, 2009: NERC submitted Version 3 of its CIP Standards to FERC for approval.

January 2010: The Operation Aurora cyber-attack was publicly disclosed by Google in January, 2010. Operation Aurora is thought to have been created by the Elderwood Group based in Beijing to gain access to and potentially modify source code repositories at high tech, security, and defense contractor companies.[51]

March 31, 2010: FERC approved final Version 3 CIP standards.

---

[49] http://usatoday30.usatoday.com/money/industries/energy/2009-04-08-power-grid-hackers_N.htm
[50] http://www.nerc.com/fileUploads/File/Events%20Analysis/A2009042101_Background.pdf
[51] http://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

April 14, 2010: Representatives Markey and Upton introduced H.R. 5026, the Grid Reliability and Infrastructure Defense (GRID) Act, a bi-partisan grid security bill. The House Committee on Energy and Commerce later approved the bill by a vote of 47-0.

June 2010: The Stuxnet computer worm, which is believed to have been designed by the United States and Israel and used in 2007 and 2010 to damage Iran's nuclear program, became public after accidently escaping from the Natanz nuclear plant in Iran, making it the first known malware that spies on and subverts industrial systems. The worm initially spread indiscriminately, but included a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes . NERC also started to develop its Version 4 CIP Standards.

June 9, 2010: The House passed H.R. 5026, the GRID Act, by voice vote. No further action was taken on H.R. 5026 during the 111th Congress and the bill did not become law.

July 2010 to September 2010: NERC sent out multiple advisories[52] to mitigate potential damage to SCADA systems as a result of the Stuxnet virus. The alert urged entities to closely review the information provided and recommended the implementation of mitigation methods.

October 13, 2010: NERC issued an alert[53] containing actionable recommendations regarding the Aurora vulnerability and requiring entities to report on progress made by December 13, 2010. The entities were required to update NERC every six months until the mitigation is completed to address any vulnerability.

February 10, 2011: NERC submitted Version 4 of its CIP Standards to FERC for approval.

February 18, 2011: NERC issued an alert[54] regarding the Night Dragon targeted cyber-attacks. Night Dragon attacks employ a combination of social engineering (used to trick a user into performing an act that provides the attacker with confidential or unauthorized access to the user's network) and well-coordinated, targeted cyber-attacks using Trojan horses, remote control software, and other malware.

April 12, 2011: FERC requested additional information from NERC on its Version 4 CIP standards proposal.

May 10, 2011: NERC issued a general alert[55] on the effects of geomagnetic disturbances and how to best mitigate their impact on the bulk power system.

---

[52] http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx
[53] http://www.nerc.com/fileUploads/File/PressReleases/PR_AURORA_14_Oct_10.pdf
[54] http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-02-18-01%20Night%20Dragon%20FINAL.pdf
[55] http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01_GMD_FINAL.pdf

September 1, 2011: The Duqu virus, thought to be related to Stuxnet, was discovered. Duqu looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive, but to gather information.

September 14, 2011: Five FERC commissioners testified[56] before the House Energy and Commerce Committee that cyber-security topped their list of threats to electric grid reliability. The commissioners agreed that the authorities provided by H.R. 5026, the GRID Act, would increase America's ability to respond to threats and vulnerabilities facing the electric grid.

September 15, 2011: FERC issued its Notice of Proposed Rulemaking to approve the Version 4 CIP standards.

October 27, 2011: Secretary of Homeland Security Janet Napolitano stated that there have been instances in which hackers came close to shutting down parts of the nation's critical infrastructure, which could potentially cause loss of life and massive economic damage[57].

December 2011: The U.S. Government Accountability Office issued a report[58] on cybersecurity finding that proper cybersecurity guidance is available but more can be done to promote its use. The report found that guidance is necessary to fully protect systems from targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

April 19, 2012: FERC approved final Version 4 CIP standards.

May 28, 2012: The existence of Flame, malware that attacks computers running the Microsoft Windows operating system, was publicly announced by multiple cyber defense teams[59]. Estimated to have been operating since February 2010, Flame attacks and spreads to computer systems over a local network or via USB stick.

June 2012: Gauss, a virus with properties similar to Stuxnet and Flame, is discovered by the Russian Kapersky Lab[60]. It appears to be intended to gather information on banking transactions and steal login information from email and social networking websites.

---

56 http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/091411%20EP%20The%20American%20Energy%20Intiative%2012%20-%20Impacts%20of%20the%20Environmental%20Protection%20Agency%27s%20New%20and%20Proposed%20Power%20Sector%20Regulations%20on%20Electric%20Reliability.pdf

57 http://www.politico.com/news/stories/1011/66988.html

58 http://www.gao.gov/assets/590/587530.pdf

59 See https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers

60 http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts

July 17, 2012: Joseph McClelland, Director of FERC's Office of Electric Reliability, testified before the Senate Energy and Natural Resources Committee[61]. McClelland stated that "[FERC's] current authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system… limitations in Federal authority do not fully protect the grid against physical and cyber threats".

July 26, 2012: General Keith Alexander, Director of the National Security Agency and the United States Cyber Command, stated that there was a 17-fold increase in cyber-attacks on American infrastructure from 2009 to 2011, initiated by criminal gangs, hackers, and other nations[62].

July 2012: The Department of Homeland Security reported[63] that cyber threats disclosed by U.S. energy companies, public water districts, and other infrastructure facilities increased over four-fold from 2010 to 2011. The Industrial Control Systems Cyber Emergency Response Team said that it received 198 reports of suspected cyber incidents or security threats in 2011.

August 16, 2012: Shamoon, a computer virus that attacks computers running the Microsoft Windows "NT" line of operating systems, was discovered[64]. The virus has been used for cyber espionage in the energy sector and is unique for having differing behavior from other malware cyber espionage attacks.

September 6, 2012: FERC Chairman Jon Wellinghoff testified that federal agencies lack the authority to properly respond to threats from known cyber-attacks and recommended that Congress provide the appropriate authority to a federal agency[65].

September 19, 2012: FBI Director Robert Mueller testified before Senate Committee on Homeland Security and Government Affairs,[66] stating that cyber security may become the FBI's highest priority in the years to come.

September 2012 to October 2012: Multiple reports of an increasing number of cyber-attacks targeting the international energy market emerged over this time period[67]. The best known of these attacks was a Shamoon attack conducted against Saudi Arabia's national oil company, Aramco. While the attack failed to disrupt oil production, it is considered one of the most destructive hacker strikes against a single business.

---

[61] http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=142d2c6c-e7e3-4b3b-9084-c7ef4ab4b88c
[62] http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=3&
[63] http://in.reuters.com/article/2012/07/03/cybersecurity-infrastructure-idINL2E8I3EAU20120703
[64] http://www.seculert.com/blog/2012/08/shamoon-two-stage-targeted-attack.html
[65] http://www.hsgac.senate.gov/media/ferc-chairman-says-electric-grid-natural-gas-lines-are-vulnerable-to-cyber-attack-
[66] http://www.fbi.gov/news/testimony/homeland-threats-and-agency-responses
[67] http://securityaffairs.co/wordpress/8951/malware/cyber-espionage-on-energy-sectorchinese-hackers-are-not-the-only.html

October 11, 2012: Secretary of Defense Leon Panetta spoke of the importance of cybersecurity and the threats it may pose to the Business Executives for National Security[68]. In his remarks, the Defense Secretary stated that "A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation."

October 18, 2012: FERC issued a Notice of Proposed Rulemaking[69] which proposed to direct NERC to submit for approval reliability standards to address the impacts of Geomagnetic Disturbances on the bulk power system.

October 2012: The Wall Street Journal reported[70] that a recent increase in cyber-attacks by the Iranian government could lead to what some officials call a low-grade cyber war.

December 2012: DHS revealed an "alarming rate" of increase in attacks against power, water, and nuclear systems in fiscal year 2012[71]. In fiscal year 2012, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 198 cyber incidents as reported by asset owners and industry partners, with 41% of these attacks being against the energy sector.

January 31, 2013: NERC submitted Version 5 of its CIP Standards to FERC for approval.

February 12, 2013: President Obama issued an Executive Order on Improving Critical Infrastructure Cybersecurity[72]. The Executive Order recognizes the threat of cyber security and the challenges it places on multiple sectors, and directs federal agencies to work with each other and industry to mitigate the threat.

February 19, 2013: The computer security firm Mandiant linked years of cyber-attacks on American corporations, organizations, and government agencies to the Chinese military[73]. The group responsible for the cyber-attacks has an increased focus on companies involved in the critical infrastructure of the United States.

March 13, 2013: FBI Deputy Assistant Director John Boles testified before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary. Mr. Boles stated that some of the most critical threats facing the United

---

[68] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
[69] http://www.ferc.gov/whats-new/comm-meet/2012/101812/E-2.pdf
[70] http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html
[71] http://thehill.com/blogs/e2-wire/e2-wire/277045-dhs-energy-sector-target-of-40-percent-of-cyber-attacks
[72] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[73] http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=1&_r&_r=0

States are from the cyber realm and highlighted the power grid as being one of the most appealing targets[74].

April 18, 2013: FERC issued its Notice of Proposed Rulemaking to approve the Version 5 CIP standards.

May 6, 2013: Middle East and North Africa-based criminal hackers launched OpUSA, cyber-attacks directed towards high-profile U.S. government agencies, banks, and other companies[75]. The Department of Homeland Safety warned against the attacks, which are considered particularly dangerous as they represent a developing alliance between criminal hackers and violent Islamic extremists.

May 09, 2013: The Department of Homeland Security's ICS-CERT released an advisory warning of a heightened risk of a potentially devastating cyber-attack against United States infrastructure[76]. The warning cited "increasing hostility" toward "United States critical infrastructure organizations."

May 16, 2013: FERC ordered NERC to develop reliability standards to address Geomagnetic Disturbances.

[74] http://www.fbi.gov/news/testimony/investigating-and-prosecuting-21st-century-cyber-threats
[75] http://www.washingtontimes.com/news/2013/may/6/jihadis-and-hackers-teaming-launch-cyberattacks-us/
[76] http://articles.washingtonpost.com/2013-05-09/world/39139314_1_senior-u-s-oil-and-gas-companies-iran

Appendix C: Additional Information about Utility Cyber-Security Personnel and Screening Policies

Utilities were asked, for each of the past 5 years, how many employees have a primary responsibility of protecting the utility against cyber-attacks.

Of the twenty-eight IOUs that responded to the question, eleven provided a numeric response to the question, but only five provided numeric responses for more than one year. Four IOUs either utilized outside vendors/contractors or supplemented their own cyber-security staff with outside vendors/contractors. Several IOUs reported dramatic increases in the numbers of cyber-security employees over the past five years, with increases of 5 to 30 employees and "up 300%" reported.

Of the twenty-one municipally- or cooperatively- owned utilities that responded to this question, eleven provided a numeric response to the question, but only two provided numeric responses for more than one year. The responses to this question that were provided by these utilities were generally less specific and informative than those provided by IOUs.

Of the eleven federal entities that own major pieces of the bulk power system, none provided numeric responses for more than one year, and few provided specific information at all.

It appears from the responses that larger investor-owned utilities are more likely to have dedicated cyber-security teams, as well as more likely to have increased their cyber-security efforts in recent years. Additional details are available in Table 2.

Table 2: Numbers of employees performing primarily cyber-security duties

	"enough" or "many"	0	1-5 employees	6-10 employees	11-15 employees	16-30 employees	31-50 employees	More than 100
# IOUs	13	0	6	4	1	2	1	1
# municipally- or cooperatively-owned utilities	12	1	5	0	1	1	0	0
Federal entities	3	6	0	0	1	0	0	0

Table 4: List of utilities that failed to respond to the request for grid security information submitted by Reps. Markey and Waxman

Name of Organization	Type of Organization
AES Corporation	IOU
Alaska Electric Light and Power Company	IOU
ALLETE	IOU
Bangor Hydro Electric Company	IOU
CH Energy Group, Inc.	IOU
Cleco Corporation	IOU
Consolidated Edison, Inc.	IOU
Enel Green Power North America	IOU
Great Plains Energy, Inc.	IOU
MDU Resources Group, Inc.	IOU
Mt. Carmel Public Utility Company	IOU
NextEra Energy, Inc.	IOU
NorthWestern Energy	IOU
NV Energy	IOU
OGE Energy Corporation	IOU
Ohio Valley Electric Corporation	IOU
Pinnacle West Capital Corporation	IOU
PPL Corporation	IOU
SCANA Corp.	IOU
Unitil Corporation	IOU
Arkansas Valley Electric Cooperative	Muni/Co-Op
Basin Electric Power Cooperative	Muni/Co-Op
Blue Ridge Electric Member Corp.	Muni/Co-Op
Bluebonnet Electric Coop	Muni/Co-Op
Bryan Texas Utility	Muni/Co-Op
Buckeye Power	Muni/Co-Op
Burbank Water and Power	Muni/Co-Op
City of Cleveland Department of Public Utilities	Muni/Co-Op
City of Denton Power Utility	Muni/Co-Op
City of Farmington Electric Utility	Muni/Co-Op
City of Riverside Utilities	Muni/Co-Op
City of Tallahassee Utility	Muni/Co-Op
City of Vernon Electric Department	Muni/Co-Op
Colorado River Commission of Nevada	Muni/Co-Op
CPS Energy (City of San Antonio)	Muni/Co-Op
Dalton Utilities	Muni/Co-Op
Electric Cooperatives of Arkansas	Muni/Co-Op
Fayetteville Public Works Commission	Muni/Co-Op
Fort Collins Light and Power	Muni/Co-Op
Grays Harbor PUD	Muni/Co-Op
Great River Energy	Muni/Co-Op
Guadalupe Valley Electric Coop	Muni/Co-Op
Holy Cross Electric Association	Muni/Co-Op
Intermountain Electric	Muni/Co-Op
Kansas City Board of Electric Utilities	Muni/Co-Op
Lafayette Utilities Commission	Muni/Co-Op
Lansing Board of Water and Light	Muni/Co-Op
Lea County Electric Cooperative	Muni/Co-Op
Lincoln Electric System	Muni/Co-Op
Long Island Power Authority	Muni/Co-Op

Lubbock Power and Light	Muni/Co-Op
Midwest Energy Inc.	Muni/Co-Op
Municipal Electric Association of Georgia	Muni/Co-Op
New Braunfels Utilities	Muni/Co-Op
Ocala Utility Services	Muni/Co-Op
Rochester Public Utilities	Muni/Co-Op
Santee Electric Coop	Muni/Co-Op
Singing River Electric Power Assoc.	Muni/Co-Op
South Texas Electric Coop	Muni/Co-Op
Tri state generation and transmission association	Muni/Co-Op
Walton EMC	Muni/Co-Op

Table 5: List of utilities whose response to the request for grid security information submitted by Reps. Markey and Waxman was incomplete or non-responsive

Name of Organization	Type of Organization
Bonneville Power Administration	Federal
Southwestern Power Administration	Federal
Western Area Power Administration	Federal
American Electric Power, Inc.	IOU
Arizona Public Service Company	IOU
Avista Corporation	IOU
Calpine	IOU
CenterPoint Energy, Inc.	IOU
CMS Energy Corporation	IOU
DTE Energy Company	IOU
Duke Energy Corporation	IOU
Duquesne Light	IOU
Empire District Electric Company	IOU
Energy Future Holdings	IOU
Exelon Corporation	IOU
FirstEnergy Corp.	IOU
Integrys Energy Group	IOU
ITC Holdings Corp.	IOU
MidAmerican Energy Holdings Company	IOU
NiSource Inc.	IOU
Northeast Utilities	IOU
NRG	IOU
Otter Tail Corporation	IOU
PG&E Corporation	IOU
Public Service Enterprise Group, Inc.	IOU
Puget Sound Energy, Inc.	IOU
Sempra Energy Utilities	IOU
Southern Company	IOU
TECO Energy, Inc.	IOU
UIL Holdings Corporation	IOU
UNS Energy Corporation	IOU
Westar Energy Inc.	IOU
Xcel Energy Inc.	IOU
Brownsville Public Utilities Board	Muni/Co-Op
Chelan County PUD	Muni/Co-Op
City of Garland Power and Light	Muni/Co-Op
City Utilities of Springfield, MO	Muni/Co-Op
Gainesville Regional Utilities	Muni/Co-Op
Independence Power and Light	Muni/Co-Op
JEA	Muni/Co-Op
Lakeland Electric	Muni/Co-Op
Modesto Irrigation District	Muni/Co-Op
Salt River Project	Muni/Co-Op
Santee Cooper	Muni/Co-Op
Silicon Valley Power (City of Santa Clara, CA)	Muni/Co-Op
Springfield, IL City Water Light and Power	Muni/Co-Op
Blue Ridge Electric Coop	Muni/Co-Op*
Brazos Electric Coop	Muni/Co-Op*
Citizens Electric Corp.	Muni/Co-Op*
East Kentucky Power Cooperative	Muni/Co-Op*

Magic Valley Electric Cooperative	Muni/Co-Op*
North Star Electric Cooperative, Minnesota	Muni/Co-Op*
Old Dominion Electric Cooperative	Muni/Co-Op*
PNCG Power, Oregon, Washington< Idaho, Montana, Wyoming, Utah, Nevada	Muni/Co-Op*
Seminole Electric Coop	Muni/Co-Op*
South Mississippi Electric Power Association	Muni/Co-Op*
Wabash Valley Power Association	Muni/Co-Op*
Withlacoochee River Electric Cooperative, Inc, Florida	Muni/Co-Op*
Wolverine Power Supply Cooperative	Muni/Co-Op*

* Signed the NRECA Letter, and did not send individual response

Table 6: List of utilities whose response to the request for grid security information submitted by Reps. Markey and Waxman was complete

Name of Organization	Type of Organization
US Army Corps Southwestern Division	Federal
US Army Corps Great Lakes and Ohio River Division, Detroit District	Federal
US Army Corps Great Lakes and Ohio River Division, Nashville District	Federal
US Army Corps South Atlantic Division	Federal
US Army Corps Mississippi Valley Division	Federal
US Army Corps Northwestern Division	Federal
Bureau of Reclamation	Federal
Tennessee Valley Authority	Federal
Alliant Energy Corporation	IOU
Ameren Corporation	IOU
American Transmission Company LLC	IOU
Black Hills Corporation	IOU
Direct Energy	IOU
Dominion	IOU
Dynegy	IOU
Edison International	IOU
El Paso Electric Company	IOU
Electric Energy, Inc.	IOU
Entergy Corporation	IOU
Green Mountain Power Corporation	IOU
Hawaiian Electric Industries, Inc.	IOU
Iberdrola USA	IOU
IDACORP, Inc.	IOU
MGE Energy, Inc.	IOU
National Grid	IOU
Pepco Holdings, Inc.	IOU
PNM Resources, Inc.	IOU
Portland General Electric	IOU
UGI Corporation	IOU
Vectren Corporation	IOU
Vermont Electric Power Company, Inc.	IOU
Wisconsin Energy Corporation	IOU
Alabama Municipal Electric Authority	Muni/Co-Op
Austin Energy	Muni/Co-Op
City of Roseville Electric	Muni/Co-Op
City of Takoma Power	Muni/Co-Op
Colorado Springs Utilities	Muni/Co-Op
Columbia Water and Light	Muni/Co-Op
Eugene Water and Electric Board	Muni/Co-Op
Imperial Irrigation District	Muni/Co-Op
Kissimmee Utility Authority	Muni/Co-Op
Los Angeles Department of Water and Power	Muni/Co-Op
Loup Power District	Muni/Co-Op
Nebraska Public Power District	Muni/Co-Op

New York Power Authority	Muni/Co-Op
North Carolina Eastern Municipal Power Agency	Muni/Co-Op
Omaha Public Power District	Muni/Co-Op
Orlando Utilities Commission	Muni/Co-Op
Pasadena Water and Power	Muni/Co-Op
Platte River Power Authority	Muni/Co-Op
PUD No 2 of Grant County	Muni/Co-Op
Sacramento Municipal Utility District	Muni/Co-Op
Seattle City Light	Muni/Co-Op