

**Congress of the United States**  
**Washington, DC 20515**

January 17, 2013

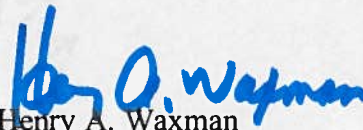
To Whom It May Concern:

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](mailto:michal.freedhoff@mail.house.gov)) or Jeff Baran (Rep. Waxman, 202-225-4407 or [jeff.baran@mail.house.gov](mailto: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?