Critical Infrastructure Security Annual Report

Commission Staff respectfully request that the company submit a Critical Infrastructure Security Report in the same docket at its 2013 reliability report by Friday, September 19, 2014. This Critical Infrastructure Security Report should include data from calendar year 2013. The company may supplement this report with available data or information from calendar year 2014, but Staff intends for annual reporting to begin on a calendar-year schedule. The report should follow the outline below.

Whenever appropriate, the term Critical Infrastructure Security (CI Security) includes unauthorized actions related to cybersecurity and physical security.

Commission Staff does not anticipate that any of the information provided in this report would be sensitive or confidential. If the response would result in providing such information, please provide a response that describes the information in a non-confidential or sensitive manner.

If you have any questions regarding the contents of this report, please do not hesitate to contact Commission's Critical Infrastructure Security team.

<u>Critical Infrastructure Security – (Cybersecurity and Physical Security)</u>

1. Critical Infrastructure Security Policy and Teams
    a. In the first report, please provide a copy of the company's CI Security policy. In subsequent reports, please provide copies of any sections of the policy that have been added or modified since the last report.
    b. Please provide an organizational diagram of the company's CI Security team(s). The diagram, or accompanying list, should include the names and titles of staff on the team, including any vacant positions or staff in acting roles.
    c. Please provide a written description of any changes made in the past year to the company's CI Security policy, and any changes to the team structure or the placement of the team in the company's organizational structure.
2. Please describe the company's participation in regional or national tabletop exercises, conferences, committees, or other events related to CI Security.
3. Please include a list of any unauthorized actions related to cybersecurity and physical security that have occurred since the last report which led to one or more of the following:
    i. loss of service;
    ii. interruption of a critical business process;
    iii. breach of sensitive business or customer information; or
    iv. serious financial harm.

    The list should include the following information about each event:
    a. any organizations or government entities notified of the event or involved in the response to the event;
    b. a description of the event and its impact;
    c. how many follow-up actions were identified as a result of the incident;
    d. how many of the follow-up actions identified in part (c.) are scheduled (please provide the calendar quarter of projected start and completion dates), in active

implementation (please provide the calendar quarter of the projected completion date), or completed; and
    e. date the incident was resolved, if applicable.
4. Does the company have retainers or contracts for outside help in the event of an incident? What kind of support is provided by the company's incident response retainers or contracts that provide similar services? Is the company currently participating in any resource sharing agreements such as the Northwest Mutual Assistance Agreement, Western Region Mutual Assistance Agreement, or Spare Transformer Equipment Program?
5. Please identify the risk assessment tools used by the company that relate to CI Security (i.e., ES-C2M2, NIST Framework, etc.).
    a. Has an independent third party reviewed the company's risk management policy?
    b. If so, who performed the review, when did it occur, and how many follow-up actions were identified? How many of these follow-up actions are scheduled (please provide the calendar quarter of projected start and completion dates), in active implementation (please provide the calendar quarter of the projected completion date), or completed?
6. Does the company have an incident response plan? If so, when was it most recently used or tested, and what is the timeframe for the next scheduled test?
7. Please describe any voluntary security standards that the company has adopted.

<u>Critical Infrastructure Security - Cybersecurity</u>

8. If available, please provide the percentage of the company's entire IT budget spent on cybersecurity. If unavailable, please provide an explanation.
9. Please provide the date of the company's most recent vulnerability assessment, who performed the assessment, and how many follow-up actions were identified. How many of these follow-up actions are scheduled (please provide the calendar quarter of projected start and completion dates), in active implementation (please provide the calendar quarter of the projected completion date), or completed?
10. Please provide the date of the company's most recent penetration test, who performed the test, and how many follow-up actions were identified. How many of these follow-up actions are scheduled (please provide the calendar quarter of projected start and completion dates), in active implementation (please provide the calendar quarter of the projected completion date), or completed?
11. Please provide the timeframe for the company's next planned vulnerability assessment and penetration test and if the company or a third party will perform each.

12. For the following information-sharing and collaboration efforts, please provide a description of the company's level of involvement with each, and complete the table below.

	Was the company involved in the effort during the calendar year?	Did the company receive alerts or information from this effort during the calendar year? If so, how often (monthly, quarterly, etc) was information from this source received and reviewed by the company?	Has the company contributed information to this effort during the calendar year?
Electricity Sector Information Sharing and Analysis Center (ES-ISAC)			
Cybersecurity Risk Information Sharing Program (CRISP)			
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)			
Seattle FBI Cyber Task Force's FLASH Alerts			
Public, Regional Information Security Event Management (PRISEM)			
Cyber Incident Response Coalition for Analysis Services, (CIRCAS)			
Other information sharing networks.			