Critical Infrastructure Security Annual Report

2013

CONTENTS

CRITICAL INFRASTRUCTURE SECURITY ANNUAL REPORT

This Report is meant to be responsive to the Commission Staff request for a Critical Infrastructure Security Report covering the year 2013. The Company has also supplemented the Report with 2014 information where requested.

1.1 CRITICAL INFRASTRUCTURE SECURITY – (CYBERSECURITY AND PHYSICAL SECURITY)

1.1.1 Critical Infrastructure Security Policy and Teams

1.1.1.1 Critical Infrastructure Security Policy

"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."

Avista considers its Security Policy an internal document and not for public distribution. While much of the information provided in the report contains high level policy statements that are not potentially damaging, there are certain sections that contain detail on Avista's actual security standards. Avista would be happy to review the document and discuss its details during a nonpublic review session. The Company's Security Policy was approved by Avista's Enterprise Security Committee. This committee is made up of directors and managers from across the different lines of business at Avista. The policy is reviewed periodically to ensure it continues to meet Avista's needs. The following is an outline of the Security Policy:

Introduction and Scope
- Introduction
- Scope

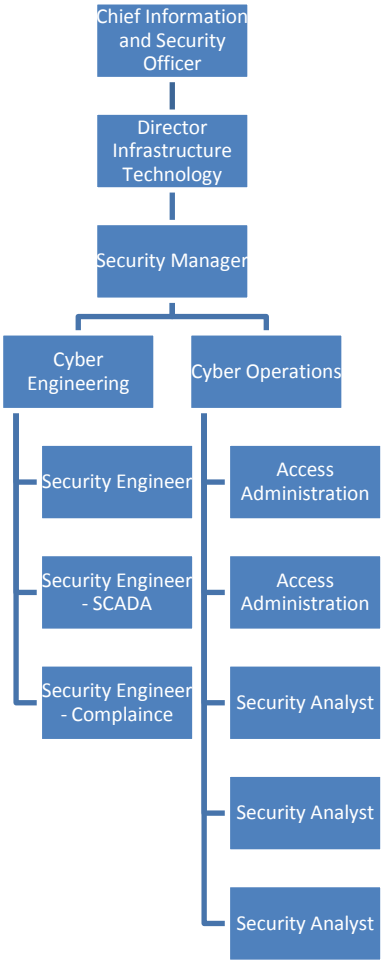
Exceptions to the Cyber Security Policy
Security Risk Management
Security Awareness
Incident Response Management
Information Management
- 100 - Physical Security Policy
- 100 - Policy Objective
- 100 - Policy Statements
- 100.1 Physical Security
- 200 - Exception Request Policy
- 200 - Policy Objective
- 200 - Policy Statements
- 200.1 Exception Request Policy

1.1.1.2 Critical Infrastructure Security Team

"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."

Provided below is a diagram of the Company's cyber security structure through 2013. In 2014, a full time position was added for physical security under the Security Manager and that will be shown in the 2014 Annual Report.

This following diagram shows actual reporting relationships and the titles of Avista Employees. The individuals names are not included because this is a public document and cyber security attacks such as phishing often originate from public information.



1.1.2 Critical Infrastructure Security Policy and Teams Changes

1.1.2.1 Critical Infrastructure Security Policy Changes

"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."

No changes were made to Avista's Security Policy in 2013.

1.1.2.2 Critical Infrastructure Security Team Changes

"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."

There were two major changes that happened in 2013. First, the responsibility for cyber and physical security where merged together under the Chief Security Officer. Second, Avista converted contractors to employees for its cyber security operations. During this conversion process, three individuals were converted from contractors to employees and two vacant positions where filled.

1.1.3 Avista's External Participation

"Please describe the company's participation in regional or national tabletop exercises, conferences, committees, or other events related to CI Security."

Avista is an active participant in many events related to Critical Infrastructure Security. Below is a list of committee's and conferences that Avista participated in during 2013 along with the frequency of event:

- EEI Security Committees (bi-monthly)
- AGA Security Committee (monthly)
- Joint EEI/AGA security conference (bi-annually)
- North American Security Working Group (monthly)
- Washington State Cyber Security Summit 2 (annually)
- DHS ONG/ Chemical Sector Threat Telebreifing (monthly)
- UTC Security Committee (monthly)
- WECC Physical Security Working Group (bi-annually)
- NERC GridSec Conference (annually)
- WECC CIPUG (bi-annually)

In addition, Avista participated in Cyber Storm IV. The purpose of this event was to assess and strengthen cyber preparedness; examine incident response processes in response to ever-evolving threats, and enhance information sharing among federal, state, international and private sector partners. The exercise design promoted more focused exercise activities, allowing participants to dive deeper into particular cyber issues. Avista actively collaborated with the Department of Homeland Security in the design and execution of this exercise. Observations and findings from this exercise informed the National Level Exercise planning activities as well as Washington State's ongoing resilience efforts.

1.1.4 Unauthorized actions related to cybersecurity and physical security

"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;*
iv. *or serious financial harm."*

Avista did not experience any unauthorized actions related to cyber or physical security events that lead to a loss of service, interruption of business processes, breach of sensitive information, or serious financial harm.

1.1.5 Incident Response

"Does the company have retainers or contracts for outside help in the event of an incident?"

Avista has a number of third parties that we do business with on a regular basis. All of these vendors have current contracts and if Avista needed help in the event of an incident, we would be able to execute a work authorization in a short amount of time.

What kind of support is provided by the company's incident response retainers or contracts that provide similar services?

The support would be tailored to the type of incident that Avista is dealing with. The main thing is having the Master Service Agreement in place so the work authorization can be executed for the type of services Avista needs at that time.

Is the company currently participating in any resource sharing agreements such as the Northwest Mutual Assistance Agreement (NMAA), Western Region Mutual Assistance Agreement (WRMAA), or Spare Transformer Equipment Program?

Avista has four Mutual Aid Agreements. Two are with WEI (WRMAA, NMAA) and the other two are with the Edison Electric Institute and the American Gas Association. In addition, Avista is a member of the EEI STEP program, which provides for the use of shared transformers in the

event of an act of terrorism and annually takes part in an exercise which allows us to evaluate a mock event and the required response.

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?

Avista has multiple incident incident response plans. The most recent test was during the Cyber Storm Exercise which was discussed in section 1.1.3. Avista's next scheduled test is scheduled for 2014.

1.1.6 Risk Management

Please identify the risk assessment tools used by the company that relate to CI Security (i.e., ES-C2M2, NIST Framework, etc.).

In 2013, Avista did an assessment using the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

Has an independent third party reviewed the company's risk management policy? If so, who performed the review, when did it occur, and how many follow-up actions were identified

During 2013, Avista had a facilitated visit with the Department of Energy. During this two day visit the Company used the Electricity Subsector Cybersecurity Capability Maturity Model tool to evaluate three different areas of the business. ES-C2M2 does not identify gaps that directly lead to follow-up action items. Instead, it allows an organization to evaluate its relative maturity against cyber security practices. From there, it is up to the organization to determine their own next steps.

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?

No specific action items came out of the Department of Energy visit.

Please describe any voluntary security standards that the company has adopted.

Avista has been using COBIT for a number of years to establish internal controls. In addition, Avista's Security policy is based on NIST 800-53. Moving forward, Avista is actively involved in and monitoring the NIST Cyber Security Framework and how it will be applied to our sector.

1.2 CRITICAL INFRASTRUCTURE SECURITY – CYBERSECURITY

1.2.1 Cybersecurity budget

If available, please provide the percentage of the company's entire IT budget spent on cybersecurity. If unavailable, please provide an explanation.

Approximately 10% of Avista's IT Infrastructure budget is spent on cybersecurity. IT Infrastructure is not the entire IT budget, but certain areas of the budget do not seem relevant for this metric and therefore were excluded.

1.2.2 Cybersecurity – Vulnerability assessments

Please provide the date of the company's most recent vulnerability assessment, who performed the assessment, and how many follow-up actions were identified.

Avista's had a vulnerability assessment performed in the 3rd Quarter of 2013. Several strategic recommendations were made and Avista currently has two active projects to address some of the recommendations made by the assessor.

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?

One of the projects was already started in 2013 prior to the accessment. That project is projected to close by the end of 2014. The other project was started in the 3rd quarter of 2014 and will likely run through 2015.

1.2.3 Cybersecurity – Penetration tests

Please provide the date of the company's most recent penetration test, who performed the test, and how many follow-up actions were identified.

Avista's had a penetration test performed in the 3rd Quarter of 2013. One immediate action item was 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?

The identified action item was resolved within approximately 30 days of the test.

1.2.4 Cybersecurity – Vulnerability & Penetration (Future)

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.

Avista is continuously performing vulnerability assessments internally. In addition, Avista is scheduled to have an outside assessment performed by the end of 2014.

1.2.5 Information-sharing and collaboration efforts

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)	Yes	Sometimes daily. Briefings monthly	Yes
Cybersecurity Risk Information Sharing Program (CRISP)	N/A	N/A	N/A
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	Yes	Varies	Yes
Seattle FBI Cyber Task Force's FLASH Alerts	Yes	Yes	Yes
Public, Regional Information Security Event Management (PRISEM)	N/A	N/A	N/A
Cyber Incident Response Coalition for Analysis Services, (CIRCAS)	N/A	N/A	N/A
DHS Fusion Centers	Yes	Varies	No
American Gas Association	Yes	Varies	No