Critical Infrastructure Security Annual Report

2018

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 2018.

1.1 CRITICAL INFRASTRUCTURE SECURITY – (CYBERSECURITY AND PHYSICAL SECURITY)

1.1.1 Critical Infrastructure Security Policy and Teams

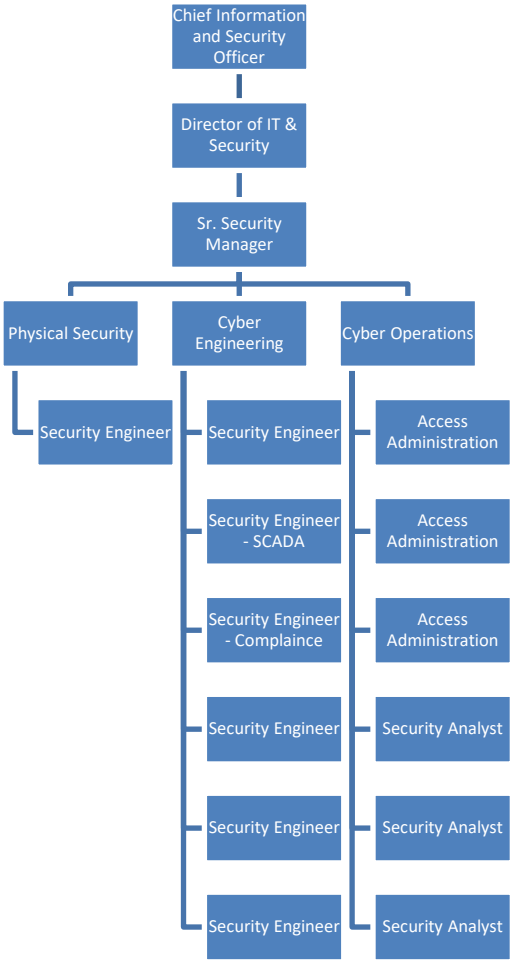
1.1.1.1 Critical Infrastructure Security Policy

Please provide a copy of the table of contents of the company's CI Security policy and identify any sections of the policy that have been added or modified since the last report.

No changes have been made.

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 titles of staff on the team.



1.1.2 Critical Infrastructure Security Policy and Team Changes

1.1.2.1 Critical Infrastructure Security Policy and Team

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.

Policy - No changes were made to Avista's Security Policy.

Organization Structure – An additional access administrator postion was added.

1.1.2.2 Security Policy Evaluation

What internal processes does the company use to evaluate its CI Security policy and structure?

Avista's security policy is generally static since it is written at a high-level. It describes the guiding principles that do not change very often rather than the "how". Avista's standards and guidelines document is constantly being updated since it describes how things must be done and because best practices are always evolving. Typically this document is updated throughout the year as our security staff identifies areas that need improvement.

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 2018 along with the frequency of event:

- EEI Security Committees (bi-monthly)
- AGA Security Committee (monthly)
- Joint EEI/AGA security conference (bi-annually)
- Washington State Cyber Security Summit (annually)
- UTC Security Committee (monthly)
- WECC Physical Security Working Group (bi-annually)
- WECC CIPUG (bi-annually)
- NERC GridSecCon (annually)
- Cyber Incident Response Coalition for Analysis Services (Varies)

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 retainiers in addition to 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?

Retainers provide service level agreements for response times. Additional support would be tailored to the type of incident that Avista is dealing through work authorizations.

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 response plans. The NERC CIP Response plans are tested annually and the Avista Data Breach Plan was tested in 2017.

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.).

Avista is currently using the NIST Cyber Security Framework and Center for Internet Security Controls for Effective Cyber Defense.

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.

Avista did not have an independent review of its use of the NIST Cyber Security Framework in 2018.

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?

Avista's security roadmap is mapped to the NIST Cyber Security Framework and is currently a 5 year plan consisting of expansion and refresh projects. Avista's would be happy to discuss or share its 5 year plan outside of a public document.

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 for Sarbanes Oxley compliance. In addition, Avista's Security policy is based on NIST 800-53.

Please describe any security training provided to Company employees.

On an annual basis, all Avista employees and contractors with cyber access are required to take security training. In addition, on at least a quarterly basis we provide security awareness by publishing relevant security articles and distribute them to all employees.

Avista also performs phishing education and testing on at least a quartlery basis. In addtion Avista provides NERC CIP specific training.

1.2 CRITICAL INFRASTRUCTURE SECURITY – CYBERSECURITY

1.2.1 Cybersecurity – Vulnerability assessments

Please provide the calendar quarter of the company's most recent vulnerability assessment. Please identify whether it was an internal or external audit, and how many follow-up actions were identified.

Avista has implemented technology to perform vulnerability assessments every night. This technology is the same as used by third parties performing vulnerability assessments. This allows us to measure our vulnerability footprint in near real-time and track progress rather than having a snapshot of vulnerability footprint once a year.

In addition Avista had two external vulnerability assessments performed by a third party in 2018.

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?

Vulnerability remediation is more operational in nature and there are not discreet projects to address vulnerabilities. Instead the work is ongoing since new vulnerabilities are published almost daily. Avista's approach is to treat vulnerability management as a continuous process and use trending to make sure we are always working on addressing all new and old vulnerabilities.

1.2.2 Cybersecurity – Penetration tests

Please provide the calendar quarter of the company's most recent penetration test. Please identify whether it was an internal or external test, and how many follow-up actions were identified.

Avista had an external penetration test performed in Q4.

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?

Follow-up actions have been priotized and will be completed in 2019.

1.2.3 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. Avista plans to have a third party vulnerability & penetration performed in 2019.

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