Contents

1. INTRODUCTION

Under the NERC functional model, ATURA POWER's Generating Stations are registered as a Generator Owner (GO) and Generator Operator (GOP) in the NPCC region within the IESO (Independent Electricity System Operator) control area. As such, ATURA POWER is accountable to protect the Bulk Electric System (BES) Cyber Systems against compromise that could lead to misoperation or instability on the BES.

ATURA POWER must be able to protect its generation facilities that contain Low Impact BES Cyber Systems against compromise through specifying select technical, operations, and procedural requirements.

2. SCOPE

This document supports ATURA POWER's Cyber Security Policy and is in accordance with CIP-003-8, requirement R2, Attachment 1, Section 3:

- Each Responsible Entity with at least one Facility identified in CIP-002-5.1a that contains Low Impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its Low Impact BES Cyber Systems.
    - ATURA POWER identifies the Halton Hills Generating Station (HHGS) and Napanee Generating Station (NGS) facilities as containing Low Impact BES Cyber Systems.
- Attachment 1, Section 3: Each Responsible Entity shall have an Electronic Access Controls plan for its generation facilities that contain Low Impact BES Cyber Systems. The Electronic Access Controls plan must be implemented to:
    - Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are:
        a) between a Low Impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing Low Impact BES Cyber System(s);
        b) using a routable protocol when entering or leaving the asset containing the Low Impact BES Cyber System(s); and
        c) not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR61850-90-5 R-GOOSE).
- Authenticate all Dial-up Connectivity, if any, that provides access to Low Impact BES Cyber System(s), per Cyber Asset capability.
    - Neither the HHGS nor NGS facilities allows dial-up connectivity.

3. DEFINITIONS

Bulk Electricity System (BES): The electrical generation resources, transmission lines, interconnections with the neighboring systems and associated equipment, generally operated at voltages of 100 kV or higher.

CIP: Critical Infrastructure Protection

DCS: Distributed Control System

Delegates: CIP-003 RCG Owner and IT Single Point of Contact

Electronic Security Perimeter (ESP): A conceptual network boundary that encloses all critical cyber assets. The ESP demarcates the high security zones of the ATURA POWER networks from the low security zones. Network traffic crossing into the ESP needs to be authenticated, monitored, and logged at the access point on the ESP.

Essential Operator's Workstations: The workstations for controlling CTG, STG, and DCS. The loss any of these workstations (and their redundancies) could cause the plant to be immediately inoperable.

RDP: Remote Desktop Protocol

SCADA: Supervisory Control and Data Acquisition

VLAN: Virtual Local Area Network

VNC: Virtual Network Computing

VPN: Virtual Private Network

4. REFERENCES

- NERC CIP-003: Cyber Security – Security Management Controls
- Halton Hills Network Design
- Napanee Network Design
- NERC Glossary of Terms

5. ACCESS CONTROLS PROCEDURE

The control network that runs and operates HHGS consists of three (3) control systems: Siemens T3000, Alstom P320 and Emerson Ovation. These three (3) control systems are logically separated and communications between each system are managed through the Emerson routers (refer to Halton Hills Network Design). Note that remote access is currently only available to Siemens.

The control network that runs and operates NGS consists of two (2) Control systems: Emerson Ovation and Mitsubishi DiaSys Netmation. (refer to Napanee Network Design). In addition, GP Strategies have access to the jump server at NGS for access to the EtaPRO application, but do not have access to any BES Cyber Systems. Note, Mitsubishi Heavy Industry (MHI) does not have remote access into the Netmation control system. MHI does however have remote access to the monitoring and data collecting system on-site through a dedicated connection but does not have access to any Low Impact BES Cyber Systems. Furthermore, NGS does have a CEMS environment that is remotely supported by CISCO and contains Low Impact BES Cyber Systems.

In order to facilitate remote support and data acquisition between the Emerson DCS and the PI Historian located on the corporate network, the SCADA network is leveraged as a secure gateway into the control DCS. The SCADA network is separated into two (2) networks or zones. The first network or zone, the DMZ (demilitarized zone) manages and facilitates all traffic between the corporate network and different control networks at the facility through jump boxes and secure data interfaces. The SCADA VLAN contains servers that facilitates user authentication and security, SCADA domain management, backups, patch management and other support and maintenance tools.

There are several levels for how remote access is managed for both ATURA POWER's support teams and external contractors. Controls are in place at each layer of ATURA POWER's network infrastructure used to manage such access.

At the corporate level, approved remote access users are provisioned corporate login credentials with membership into specific security groups that are restricted VPN connections for their team or company and the sites they can access. In addition to using their corporate credentials, each user is required to use the Microsoft Authenticator app on their phone to verify the login request. Accounts for external vendors have their account tied to the Microsoft Authenticator app on a cellphone located in the plant's control room, which will require the operator on duty to approve access. This ensures the operators are fully aware whenever a vendor connects remotely to the site.

At the SCADA level, a second set of login credentials are required. This second set of credential authenticates with ATURA POWER's SCADA domain. Such as the case with the corporate level, security group memberships are used to control which sites a user is permitted to access and which systems or assets within the site a user can connect to.

5.1. Pre-requisites for Access Requests

Following are the pre-requisites that must be verified prior to submitting a request for access to the HHGS or NGS Low Impact BES Cyber System.

- The position/job function for the person requesting access.
- The requester has the appropriate ATURA POWER security level.

- ATURA POWER employees must have approved background checks.
- The requester has completed the cyber security awareness training as per ATURA POWER's procedure on Cyber Security Awareness Training.

5.2. Access Request and Authorization

Following are the steps required to authorize electronic access to the Low Impact BES Cyber Systems located at HHGS and NGS.

1. The requester completes Section 1 of the ATURA POWER Access Request Form (see Appendix A) and submits to their manager for review and approval
2. The manager reviews the request to ensure the requester has the pre-requisites as required and completes Section 2 of the ATURA POWER Access Request Form
3. The manager approves or denies the request.

5.3. Revocation of Access

When an authorized user no longer requires electronic access to the HHGS and NGS Low Impact BES Cyber Systems, said access will be revoked as soon as possible once determined it is no longer required.

5.4. Retain Access Request Form

The completed Access Request form (see Appendix A) must be retained for three (3) years or until the next NERC audit.

6. Remote Interactive Access Controls

Apart from Siemens at Halton Hills, all vendors share a common process of using ATURA POWER's Cisco AnyConnect VPN for remotely connecting to the control systems they support. In Siemens case, a permanent B2B (business-to-business) VPN connection is used instead of the Cisco AnyConnect connection.

The following outlines the general process for connecting remotely to the controls system at a facility using ATURA POWER's Cisco AnyConnect VPN.

Note: Each external vendor approved for remote access is provided a dedicated VPN web portal for their specific company.

1. A vendor support agent initiates a VPN connection using a dedicated web portal provided to their company.
2. The support agent will be prompted with authentication challenge for ATURA POWER's corporate credentials.
3. The vendor's username and password are entered.
4. Upon a successful VPN connection, the support agent will establish a remote connection to their dedicated SCADA jump box via RDP or Horizon View (application or web portal).
5. Another password challenge will be prompted to connect to the SCADA jump box. This will require a SCADA specific account assigned to the support agent.
6. Once successfully connected to the jump box the vendor will have access to the systems and assets via RDP or VNC shortcuts on the jump box.

7. Remote Access for Siemens (User Access)

The remote access process for Siemens to the HHGS follows a similar process to the standard process for all other vendors with the exception they utilize a persistent B2B (business-to-business) VPN connection between their customer remote service platform (cRSP) and a jump box at the HHGS.

8. ADMINISTRATION OF PLAN

8.1. Document Review

This Electronic Access Controls Plan must be reviewed, updated as required, and approved at least once every 15 calendar months.

8.2. Compliance Records and Retention

- Retain each completed Appendix A – Access Request Form for three calendar years

Appendix A – Access Request Form

Section A: To be completed by the Requester/Employee				
Last Name:		First Name:		Date:
Company:	Atura: ☐	External: ☐	External Company Name:	
Department:				
Job Title:				
Manager Name:				
Access	Electronic Access	HHGS ☐	NGS ☐	

Section B: Responsible Manager Use Only			
Last Name:	First Name:		Date:
Department:			
Job Title:			
Cyber Security Awareness Training:	Completed: Yes ☐ No ☐		Date completed:
Security Clearance Completed:	Completed: Yes ☐ No ☐		Date completed:
Comments:			

Approval	
Signature:	Date: