AMERICAN TRANSMISSION COMPANY®	**Business Practice**	**Department:**	**External Affairs**
		Document No:	**BP-1601 v2.0**
Title: **PHYSICAL AND CYBER SECURITY**		**Issue Date:**	**07-02-2020**
		Previous Date:	**09-23-2016**

Contents

Approved By: **Randy Karls**	Author: **Matt Waldron**

1 PURPOSE

This Business Practice outlines the physical and cyber security measures that are implemented between ATC and its interconnected entities (IEs). The physical security systems installed at joint-use substations are coordinated installations between ATC and its IEs. Cyber security measures are in place to allow safe and secure access to ATC's computer applications used to operate and maintain the transmission grid.

2 SCOPE AND APPLICABILITY

This Business Practice includes aspects of physical and cyber security as it relates to the systems in place that affect both ATC and its IEs. Other physical and cyber security systems used solely for ATC or its IEs are not covered here. ATC continuously evaluates risk and makes changes to measures as appropriate.

2.1 Physical Security and Cyber Security

ATC's implementation of the security programs are based on:

- ATC prioritization as well as FERC and NERC requirements
- Risk assessment on a program, individual site basis which includes threats, vulnerabilities and consequences
- Installation and mitigation measures based on the risk assessment results

3 ROLES AND RESPONSIBILITIES

Regional Manager Customer Relations

- Schedules and facilitates meetings between ATC and IE
- Provides issue resolution management
- Maintains key points of contact for physical and cyber security
- May serve as ATC Sponsor to establish access to ATC sites and systems

ATC Sponsor for Contingent Worker

- Ownership of primary business relationship for Contingent Worker
- Initiates position/contract request in ATC Human Capital Management (HCM) system
    - Identifies access prerequisite needs via Job Profile selection
- Submits and approves access/provisioning requests in ATC's Identity Access Management (IAM) system
    - Provides justification for access needs
- Communicates/initiates Contingent Worker terminations to HR in event of employment status or access requirement change

ATC Contingent Worker Program Manager (CWPM)

- Processes contract/position requests
- Manages communication/outreach to Contingent Worker and identifies Points Of Contact throughout onboarding process, including relevant ATC policies and procedures
- Monitors prerequisite completion to ensure adherence to Contingent Worker Program
- Process and communicate Contingent Worker terminations to ATC stakeholders

ATC Contingent Worker

- Completes applicable prerequisites (screenings, forms, training, etc.)
- Complies with all applicable ATC policies and procedures

Point of Contact (POC)

- Works with ATC Sponsor to provide/contract CW resources

- Ensures CW candidates are completing required onboarding activities
- Acknowledges and confirms CW employment verifications
- Contacts ATC Immediately in event of CW termination of service

Visitor/Worker to ATC Sites

- Completes prerequisites prior to access
- Ensures access needs are requested and approved
- Completes weekly verification of employment status and access need (CIP)

4 EXPECTATIONS FOR ACCESS TO ATC SYSTEMS AND SITES

4.1 Acquiring Access to ATC Sites and Systems

Requests for access to ATC sites and systems are managed through ATC's Contingent Worker Program. This process is initiated by contacting the ATC Sponsor. To receive information regarding access to ATC sites, contact the ATC Regional Manager Customer Relations.

At existing sites where security upgrades impact current access procedures, Regional Manager Customer Relations works with the affected IE to begin coordination with the Contingent Worker Program Manager to ensure IE maintains access to necessary assets.

When connecting to ATC Cyber Assets or Systems, IEs are expected to use secure methods and operate in accordance with:

- ATC's Cyber Security Policy, and Appropriate Use of Electronic Resources Policy,
- Practices defined in ATC's annual Security Awareness Training,
- Onsite signage, instructional documentation, and provided hardware, if any
- Practices defined within legal contracts between ATC and the IE

4.2 Maintaining Access to ATC Sites and Systems

To maintain access to ATC Sites and Systems, an ATC Contingent Worker must complete the following actions:

- Complete required training as assigned through ATC's Contingent Worker Program
- Comply with ATC policies and procedures
- Provide notification of changes to employment status and access needs

4.3 Deactivating Access to ATC Sites and Systems

Contingent Worker deactivations and terminations are to be communicated to HR by:

- Designated Point(s) Of Contact (POC's)
  - Termination of Service (TOS) process/form submitted to ATC
- ATC Sponsor
  - Termination initiation in ATC Human Capital Management (HCM) system
  - Phone call to ATC Corporate Security hotline (after hours)

5 PROCESS FOR IMPLEMENTATION OF OR MODIFICATIONS TO SECURITY MEASURES AT A NEW OR EXISTING FACILITY

5.1 Criteria

Following asset identification and the physical security risk assessment, the effectiveness of existing security and operational practices is evaluated. Based on this evaluation, recommended actions and mitigation measures are developed that will cost effectively mitigate risks by identifying threats and reducing vulnerabilities and/or consequences for ATC and the IE. Actions may include changes to ATC and IE operational programs, policies or procedures. ATC will then develop a plan to install additional security mitigation measures as required to effectively reduce operational risk.

5.2 Initiation of Security Measures by ATC

Following an ATC site survey and risk assessment results, ATC determines an appropriate physical security package through the project development process. Discussion and collaboration with all asset owners at the site to review proposed security measures occurs following development of a preliminary project scope and schedule, adhering to the ATC project request process. At an IE-controlled site, ATC will initiate consultation with IE to discuss proposed security measures to ensure consensus on appropriate protection. Regional Manager Customer Relations communicates available project information with impacted IE.

The final design of implemented measures is determined during detailed design with input from ATC Corporate Security, ATC Asset Management and IE.

5.2.1 Cyber Security

ATC is responsible for notification of cyber security changes to the IE personnel.

5.3 Initiation of Security Measures by Interconnected Entity

At an IE-controlled site, ATC requests consultation with IE to discuss proposed security measures to ensure appropriate protection is in place. IE can contact the Regional Manager Customer Relations with proposal.

6 COST RESPONSIBILITY

6.1 Physical Security

Cost allocation for physical security measures implemented at a joint-use substation is documented in Joint Use Substations – Cost Responsibility for Common Facilities Business Practice. This Business Practice is available at:

http://www.atcllc.com/customer-relations/business-practices/

6.2 Cyber Security

IEs are not billed for ATC-initiated work for implementation of cyber security measures at a joint-use substation.

7 COMPLIANCE

Each entity is responsible for their compliance obligations. When implementing physical security measures at Joint-Use Substations, ATC will coordinate with the impacted IE.

Information shared and exchanged through the processes described in this Business Practice may be Critical Energy Infrastructure Information (CEII) and subject to ATC's Identification and Protection of CEII Materials Procedure.

8 DOCUMENT REVIEW

This document will be reviewed annually.

9 RECORDS RETENTION

Documents are maintained per the Records Retention Schedule.

Records Management Index System (RMIS)

Records Management Policy #2002-2 Revision Information

10 REVISION INFORMATION

Version	Author	Date	Section	Description
1.0	Ben Stuart	09-16-16	All	Original
2.0	Matt Waldron	07-02-2020	Expectations	Transient Cyber Assets