AMERICAN TRANSMISSION COMPANY	**Corporate Security Procedure**	**CIP** **CORPSEC-PRCD-040-0811**
Access Control Procedure for Substations with Enhanced Security		**Revision:** 00 **Issue Date:** 8/26/11
Document Classification:	*Confidential*	**Effective Date:** 09/01/11
Author:	**Linda Lowe, Security & Compliance Specialist**	8/26/11
Approver:	**Jason Shaver, System Operations Support**	8/26/11

1. Overview

1.1 Purpose

The purpose of this *procedure* is to document the requirements for access to enter the Physical Security Perimeter (PSP) of substations with enhanced security[1].

1.2 Scope

This document will provide compliance and implementation guidance for access control and visitor management requirements for substations with enhanced security.

2. Applicability

2.1 Regulatory Applicability

The requirements identified in this program are applicable for the North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) Standard CIP-006, R1.4, R1.6 and R6 to ATC as a Transmission Owner (TO) and Transmission Operator (TOP).

2.2 Affected Assets

This document is applicable for all substations designated by ATC that require a Physical Security Perimeter (PSP) for the protection of Critical Cyber Assets (CCAs) and cyber assets that control and/or monitor the Electronic Security Perimeter (ESP).

2.3 Affected Personnel

2.3.1 Corporate Security – responsible for electronic access control system and the processes and procedures for allowing gainful access.

[1] Reference *Access Control Program for the Physical Security Perimeter* (PSP) CORPSEC-PGRM-003-0911

2.3.2 ATC Employees – responsible for 1) overseeing work conducted at substations with enhanced security to ensure visitors under their control are familiar with and follow procedures; 2) complying with the access control requirements for substations with enhanced security.

2.3.3 Service Vendors – responsible for 1) overseeing work conducted at substations with enhanced security to ensure visitors under their control are familiar with and follow procedures; 2) complying with the access control requirements for substations with enhanced security.

2.3.4 Local Distribution Company (LDC) – responsible for 1) ensuring that employees that have authorized unescorted access to substations with enhanced security are familiar with and follow this procedure; 2) coordinating access requests[2]; 3) communicating terminations to ATC Corporate Security .

3. Procedures for Unescorted Access

3.1 PSP Entry – Card Access

3.1.1 To enter the PSP, the badge holder will present his or her security identification badge at the card reader.

3.1.2 Each individual entering the PSP must present his or her badge at the card reader to log their access.[3] It is important to note that when multiple persons are entering the PSP at the same time, **EACH** individual must present his or her badge at the card reader.

3.1.3 It is an infraction of ATC Policy to "tailgate" or "piggyback" on someone else's access.[4] If a mistake is made, contact ATC System Control Operations (SCO) (number listed at the entrance to the PSP) to report the infraction. This will avoid a report to the Office of Compliance for further evaluation. Failure to report an infraction, may be viewed as an "intentional action" and will require further review of the incident.

---

[2] Reference *Access Control Program for the Physical Security Perimeter* (PSP) CORPSEC-PGRM-003-0911

[3] CIP-006 R4

[4] ATC Security Access Control Policy

3.2 Access Issues – Forgotten Badges

3.2.1 If a badge holder arrives at a substation with enhanced security and has forgotten his or her badge, the individual will contact the SCO to receive a temporary PIN code.

3.2.2 The SCO will ask the badge holder for the answer to one of the "challenge" questions recorded in the physical access control (PAC) system . If the badge holder successfully answers the question, the SCO will provide the individual with a temporary 6-digit PIN code to enter at the door. This PIN code may be used during the entire visit.

3.2.3 Important: If the badge holder cannot successfully answer one of the "challenge" questions, the SCO is not authorized to grant access to the PSP. The badge holder will need to locate another individual with access privileges to the PSP to act as an "escort". It is important to note that both the escort and badge holder must follow all escorting requirements for substations with enhanced security.

3.2.4 Upon notification that a PIN code has been used, ATC Corporate Security will reset the PIN code for the badge holder's record.

3.3 Access Issues – Card Reader Malfunctions

3.3.1 In the event that the card reader is not operational, a badge holder will go to a different door and try another card reader. If all card reader(s) are not working, the individual will contact the SCO at the number listed on the door to the PSP to report the issue.

3.3.2 The SCO will ask the badge holder for the answer to one of the "challenge" questions recorded in the PAC. If the badge holder successfully answers the question, the SCO will provide the individual with a temporary 6-digit PIN code to enter at the door. This PIN code may be used during the entire visit.

3.3.3 Important: If the badge holder cannot successfully answer one of the "challenge" questions, the SCO is not authorized to grant access to the PSP. The badge holder will need to locate another individual with access privileges to the PSP to act as an "escort". It is important to note that the escort must follow all escorting requirements for substations with enhanced security.

3.3.4 Upon notification that a PIN code has been used, ATC Corporate Security will reset the PIN code for the badge holder's record.

3.4 Access Issues – System Device Failure/Emergency Key

3.4.1 In the event that the PAC system is not operational due to an electrical outage or some other reason, the SCO will need to authorize access to the "key vault". The steps are as follows:

a. The badge holder will contact the SCO who will provide the combination to the key vault. The badge holder will use the emergency key for access. The key may be used for the entire visit

b. Upon completion of the work, the badge holder is responsible for placing the emergency key back into the key vault and notifying the SCO that the key has been returned.

c. The SCO will notify Corporate Security of the device failure, provide the name(s) of the individuals that accessed the PSP, and verified that the key was returned to the vault.

d. Corporate Security will arrange repairs (if necessary) and change the combination on the key vault and audit the key vault to document that the key was returned.

4. Procedures for Visitor Control

4.1 Visitor Management

4.1.1 Escorting - All personnel that do not have authorized unescorted physical access to substations with enhanced security are considered "visitors" and must be continuously escorted.

a. Escorted personnel must be identified by the escort by the use of a company ID, driver's license or other means to ensure that the name on the log is accurate.

b. An escort must maintain visual control and awareness of their visitors and activities within the PSP.

c. The ratios of visitors to escort are:

1. 9:1 – tours/meetings
2. 5:1 – work being performed

d. Escorts may allow visitors to leave the PSP for short tasks (e.g., retrieving items from vehicles) without logging out.

e. Escorts are responsible to verify that all visitors are logged out of the PSP when they leave the site by entering the "exit" time in the visitor register.

4.2 Logging

4.2.1 All visitors entering the PSP must be logged into the Visitor Register.

4.2.2 The Visitor Management Register is located in a defined binder within the PSP. To properly register the visitor, the following information must be legibly completed on the paper log. (see sample log on attachment A)

a. Visitor Name

b. Date of Visit

c. Reason for visit

d. Escort Name

e. Escort Signature

f. Time In

g. Time of Exit

4.2.3 At the end of the visit, the Escort must finish completing the log by recording the time out.

4.3 Visitor Log Records Management

4.3.1 Visitor Logs

a. The completed log forms will be collected regularly during the substation inspection process.

b. If there are no entries for the month, the inspector will draw a line across the document, indicate "no entries" and sign the document.

c. It will be the responsibility of the inspector to:

1. Scan/email the paper logs to: atcsecurity@atcllc.com

2. Mail the originals to: ATC Corporate Security, P.O. Box 47, Waukesha, WI 53188.

d. ATC Corporate Security will review the logs and file the electronic copy for record purposes.

e. Logs will be retained for a minimum of 90 days after the review.

f. Logs associated with a possible incident will be archived for a minimum of three (3) years following the end of the investigation.

5. Procedures for Special Projects

5.1 PSP Access Points

5.1.1 If during a special projects at substations with enhanced security, the PSP access points need to be propped open, at any time, the project will need to assign a **dedicated** door monitor stationed at a PSP access point to monitor and log access.

5.1.2 One (1) **dedicated** door monitor is required for each PSP access point that will be propped open.

5.1.3 The **dedicated** door monitor may not leave their post, at any time, while the door is propped open.

5.1.4 PSP access points may not be propped open at any time, for any amount of time, without a **dedicated** door monitor assigned to monitor and log access.

5.1.5 Any projects involving the PSP should be coordinated, in advance, with ATC Corporate Security in order to review the responsibilities of the door monitor and logging process.

6. Supporting Information

6.1 Definitions

6.1.1 Physical Security Perimeter Access Point – Doors, windows and other openings through the six wall perimeter that exceed 96 sq. inches with a minor dimension of 6" with deflection criteria of <1/2' in a 9' span.

6.1.2 Physical Security Perimeter – The physical, completely enclosed ("six-wall") border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which critical cyber assets are housed and for which access is controlled, as defined by NERC.

6.2 Sample Forms

6.2.1 Attachment A – Visitor Management Register

6.3 Reference Documents

6.3.1 ATC Security Access Control Policy

6.3.2 ATC Cyber Security Policy

6.3.3 CORPSEC-PGRM-003-0911 Access Control Program for the Physical Security Perimeter (PSP)

7. Administration

7.1 APPLICABLE NERC, MRO, AND RFC STANDARDS

7.1.1 North American Electric Reliability Corporation (NERC) – Cyber Security - Physical Security of Critical Cyber Assets (CIP-006)

7.2 Data Retention

7.2.1 Refer to Sections 4.3.1c and 4.3.1d.

8. Review and Revision History

8.1 Periodic Review

On an annual basis, this *Procedure* shall be reviewed and revised in accordance with the *ATC Cyber Security Policy*.

8.2 Revision History

Revision Number:	Reason:	Author/ Reviewers:	Approved by:	Effective Date:
00	Procedure Creation	Linda Lowe, Corporate Security Team, SCO Supervisors	Jason Shaver	9/01/11

9. Appendix A – Visitor Management Register *(Sample Form)*

INSTRUCTIONS TO ESCORTS:
1. Visitors must be registered by the Escort.
2. Each visitor must be properly logged on this form.
3. Complete each column of the Register.

VISITOR MANAGEMENT REGISTER
Site

			Date Log Started			
DATE OF ENTRY (M/D/YY)	VISITOR NAME (Please print - First Name/Last Name)	REASON FOR VISIT	ESCORT NAME (Please Print - First Name/Last Name)	ESCORT SIGNATURE	TIME IN	TIME OF EXIT

Note to Inspectors: This form must be scan/emailed to atcsecurity@atcllc.com following routine inspection visits.

Form CSxxxx (dated x/xx/xx)

This Visitor Register is the property of ATC.