Policy Owners:	EVP Gen Counsel & Corp Secretary
Original Issue Date:	06/30/2008
Revision Number:	17
Revised Effective Date:	01/01/2023
Approved By:	CIP Senior Manager, & Policy and Ethics Committee

NERC CIP CYBER SECURITY POLICY
[CIPPOL-03008-NERC CIP Cyber Security Policy]

PURPOSE

This Policy defines American Transmission Company's, LLC (ATC) commitment to identify and protect its Bulk Electric System (BES) Cyber Assets/Systems identified as essential to the reliable operation of ATC's impact-rated BES Facilities/Assets, and which are protected in accordance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cyber Security Standards in order to support safe, secure, reliable operation of the BES.

SCOPE

ATC BES Cyber Assets/Systems, as well as any Cyber Assets and information meeting the criteria for NERC CIP protection in accordance with the Applicable Systems criteria, must be managed and protected in accordance with this Policy and any associated or referenced programs, procedures, standards, and documents.

Personnel who have been granted authorized cyber or authorized unescorted physical access to ATC's BES Cyber Assets/Systems, as well as any Cyber Assets and information meeting the criteria for NERC CIP protections, including, but not limited to, employees and contingent workers, are governed by this Policy and shall also comply with any associated or referenced programs, procedures, guidelines, and documents.

DEFINITIONS

For the definition of terms used in this Policy and other documentation related to the NERC CIP Standards, refer to the ATC NERC CIP Glossary of Terms.

ATC COMMITMENT

This policy defines three broad commitments to compliance with the NERC CIP Cyber Security Reliability Standards.

- As an owner and operator of electric transmission system facilities, ATC supports the stability of the BES by providing reliable electric transmission services to its customers, and adherence to regulatory obligations is part of that mission.

– A commitment to secure BES Cyber Assets/Systems through adherence to the NERC CIP Standards extends to all personnel throughout the Company organizational structure, up to and including the CIP Senior Manager, the officers of the Company, and the corporate Board of Directors.

– The NERC CIP Cyber Security Reliability Standards provide a cyber-security framework for the identification and protection of ATC's in scope Cyber Assets/Systems and ATC programs are as follows:

CIP-002 – BES Cyber System Categorization

Assures the identification, documentation, and review of the High, Medium, and Low impact-rated BES Cyber Assets/Systems at and/or associated with the impact-rated BES Facilities/Assets that are identified and categorized through the application of the impact-rating criteria in CIP-002 Attachment 1.

CIP-003 – Security Management Controls

Assures that Responsible Entities have documented security management controls (e.g. governance; policies; leadership designations and authority delegations;declaration of and response to CIP Exceptional Circumstances) in place to protect BES Cyber Assets/Systems and Information as pertinent to the identified impact-rating and categorization.

CIP-004 – Personnel & Training

Assures that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Assets/Systems, including contingent workers, have the prerequisite and required ongoing level of personnel risk assessment, training, and security awareness appropriate to individual roles, functions, or responsibilities. Specific controls are prescribed for the review, management, provisioning, and revocation of cyber or unescorted physical access to BES Cyber Assets/Systems, accounts, and electronic and physical BES Cyber Asset/System Information or designated storage locations as pertinent to the listed Applicable Systems.

CIP-005 – Electronic Security Perimeter(s)

Assures the identification and documentation of the electronic perimeter(s) protecting BES Cyber Assets/Systems, as well as any access points to the perimeter, any Protected Cyber Assets inside the perimeter, and those Cyber Assets/Systems used in the electronic access control and/or monitoring of the perimeter or BES Cyber System. Specific controls are prescribed for electronic perimeters, access points, Cyber Assets used for electronic access control and/or monitoring, physical access control, as well as for access and connectivity, including Interactive Remote Access, to and from BES Cyber Assets/Systems and perimeters as pertinent to the listed Applicable Systems, and management of vendor remote access.

CIP-006 – Physical Security of BES Cyber Systems

Assures the documentation and implementation of a physical security program for the protection of BES Cyber Assets/Systems. Specific controls are prescribed for physical perimeters, restricted areas, and physical access points, Cyber Assets used for physical access control, alerting, and/or logging of access to perimeters as well as for physical access to BES Cyber Assets/Systems, perimeters, and restricted areas as pertinent to the listed Applicable Systems.

CIP-007 – Systems Security Management

Assures the definition and documentation of methods, processes, and procedures for securing routable BES Cyber Assets/Systems, and Protected Cyber Assets within the Electronic Security Perimeter(s), as well as non-routable BES Cyber Assets/Systems as pertinent to the listed Applicable Systems. Specific controls (e.g. malware prevention, patch management, security event monitoring, system access control) are also prescribed on a BES Cyber System basis and per device capability.

CIP-008 – Incident Reporting and Response Planning

Assures the identification, classification, response, handling, and reporting of Cyber Security Incidents related to BES Cyber Assets/Systems as pertinent to the listed Applicable Systems. Specific routine preparedness activities to test plans are also prescribed.

CIP-009 – Recovery Plans for BES Cyber Systems

Assures that recovery plan(s) are put in place for BES Cyber Assets/Systems in support of the continued stability, operability, and reliability of the BES. Specific controls are prescribed for the backup and storage of BES Cyber Assets/Systems information required for recovery, the preservation and retention of data to aid in root cause analysis for detected Cyber Security Incidents, as well as specific routine preparedness activities to test plans and a representative sample of information used in recovery.

CIP-010 – Configuration Change Management and Vulnerability Assessments

Assures the development and implementation of processes and controls to authorize and manage BES Cyber Asset/System change to a known baseline configuration as pertinent to the listed Applicable Systems. Specific controls are also prescribed for the monitoring and testing of changes, verification of the identity of the software source and the integrity of the software, the identification of security controls that could be impacted by change, as well as verification of the security posture post-change. Specific routine vulnerability assessment activities as well as development and implementation of plans and controls for Transient Cyber Assets and Removable Media as pertinent to the listed Applicable Systems are also prescribed.

CIP-011 – Information Protection

Assures BES Cyber Asset/System information is identified, securely stored, transmitted, used, and handled to mitigate risks of compromising confidentiality as pertinent to the listed Applicable Systems. Specific controls are also prescribed for the prevention of unauthorized retrieval of BES Cyber Asset/System information from reuse or disposal of Applicable Systems.

CIP-012 – Communication Between Control Centers

Assures the protection of the confidentiality and integrity of Real-time Assessment and Real-Time monitoring data transmitted between Control Centers.

CIP-013 – Supply Chain Risk Management

Assures implementation of supply chain risk assessment practices and security controls from the procurement of Goods[1] or Agreements[2] (and use of associated services) relative to high and medium impact BES Cyber Systems and associated Cyber Assets as pertinent to the listed Applicable Systems to mitigate risk to the reliable operation of the Bulk Electric System (BES).

CIP-014 – Physical Security of BES Assets

Assures implementation of risk assessment & mitigation practices and security controls to identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection in support of reliable operation of the Bulk Electric System (BES).

RoP-4D – Technical Feasibility Exceptions

Assures technical infeasibilities for BES Cyber Assets/Systems, as well as any Cyber Assets and information meeting the criteria for NERC CIP protections, are identified, documented, mitigated, and managed to reduce the risk to safe, secure, reliable operations of the BES. Also prescribes the criteria for identifying and reporting Material Changes to the Midwest Reliability Organization (MRO) for Technical Feasibility Exceptions (TFEs) in accordance with the enforceable NERC Rules of Procedure (RoP) Appendix 4D.

RESPONSIBILITIES

All employees, suppliers, and contingent workers are responsible for:

- Understanding and adhering to the provisions defined in this policy
- Performing their job responsibilities in accordance with the NERC Reliability Standards
- Promptly reporting any suspected potential non-compliance with the NERC Reliability Standards, per ATC's Open Door Policy
- Developing and executing internal controls, corrective actions, and mitigation plans, as necessary

[1] Refer to the Legal Review Procurement and Expenditures Authorization Policy for the definition of "Goods".

[2] Refer to the Legal Review Procurement and Expenditures Authorization Policy for the definition of "Agreements".

Managers and subject matter experts who have been assigned accountability for NERC Reliability Standards are responsible for formulating and executing programs, procedures, and controls which assure compliance.

ATC's Reliability Standards Compliance team within the Legal department is responsible for:

- Administering corporate programs which support compliance with the NERC Reliability Standards
- Performing or facilitating independent reviews of compliance program activities
- Self-reporting any identified potential non-compliance with the NERC Reliability Standards to ATC's regulators
- Acting as ATC's primary interface with ATC's regulators
- Managing and influencing ATC's regulatory environment

ATC's Reliability Standards Compliance (RSC) program is overseen by ATC's Security, Governance, Risk, and Compliance (SGRC) Steering and Managing Committees who operate in accordance with their defined charters published on ATC's intranet.

Employees with cyber or physical access to ATC's in scope Cyber Assets/Systems are responsible for understanding and adherence to, this NERC CIP policy and the body of program documentation including, but not limited to, plans, processes, procedures, guides as well as ATC standards, definitions, and interpretions. Based on the following designations, additional responsibilities apply:

- *CIP Senior Manager* – ATC has assigned a single senior manager with overall responsibility and authority for leading and managing ATC's implementation of and adherence to Standards CIP-002 through CIP-014. The CIP Standards include annual and ad-hoc approval responsibilities for the CIP Senior Manager, and, in specifically identified requirements, the CIP Senior Manager may delegate those approval responsibilities.

- *CIP Senior Manager Delegate* – Delegates, if any, assume specified responsibilities on behalf of the CIP Senior Manager, where the standards allow delegation. Delegations are documented and approved by the CIP Senior Manager and the delegate to assure acknowledgement of the specific accountabilities being delegated.

- *Functional Manager* – While the CIP Senior Manager has overall accountability for adherence to the CIP Standards, ATC has divided the ownership of the specific compliance obligations by asset ownership and expertise. The obligations for each Functional Manager are defined and assigned within ATC's NERC CIP program documentation.

REPORTING

It is the responsibility of all ATC employees to report any suspected violations of this policy, in accordance with ATC's Open Door Policy.

EXCEPTIONS/VIOLATIONS

CIP Exceptional Circumstances to this policy require the approval of the designated NERC CIP Senior Manager.

Exceptions based on technical infeasibility require the approval of the designated NERC CIP Senior Manager, or documented delegate.

Employees who violate this policy are subject to disciplinary action, up to and including termination.

REFERENCES

- Acceptable Use of Electronic Resources Policy
- Legal Review, Procurement, and Expenditures Authorization Policy
- NERC Reliability Standards Policy
- Personnel Risk Assessment Policy
- Physical Access Control Policy
- Risk Management Policy
- Travel and Expense Policy

Program documents are incorporated via reference and can be found on PowerLine at Enterprise > ATC Standards Website > Reliability Standards Compliance

Approver(s)
Sharon Koller, Lead Compliance Strategist & CIP Senior Manager Digitally signed by Sharon Koller, Lead Compliance Strategist & CIP Senior Manager Date: 2022.11.16 14:54:55 -06'00'