NERC CIP Security Standards Policy Mapping

The following table illustrates how specific policy topic categories within ISO 27002 (*Information Security Policies Made)* map to the cyber security requirements of the Mandatory Reliability Standards for Critical Infrastructure Protection (CIP) [1] from the North American Electric Reliability Corporation (NERC).

Standard Number	Description	ISO 27002
CIP-002-4	**Critical Cyber Asset Identification**	7 ASSET MANAGEMENT
	Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.	
R1. Critical Asset Identification Method	The Responsible Entity (RE) shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	6.1.2 Information Security Coordination 6.1.1- 2. Risk Assessments 6.2.1 Identification of risks related to external parties 14.1.2 Business continuity and risk assessment 15.1.1- 6. System Risk Assessments
R2. Critical Asset Identification	The RE shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The RE shall review this list at least annually, and update it as necessary.	7.1 RESPONSIBILITY FOR ASSETS. 7.1.1 Inventory of assets 7.1.2 Ownership of assets 7.1.3 Acceptable use of assets
R3. Critical Cyber Asset Identification	Using the list of Critical Assets developed pursuant to Requirement R2, the RE shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.	7.2 INFORMATION CLASSIFICATION 7.2.1 Classification guidelines 7.2.2 Information labeling and handling
R4. Annual Approval	A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets.	15.2.1 Compliance with security policies and standards. 15.2.2 Technical compliance checking
CIP–003–4	**Security Management Controls**	
	Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.	
R1. Cyber Security Policy	The RE shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.	5.1.1 Information Security Policy Document 5.1.2 Review of the information security policy
R2. Leadership	The RE shall assign a senior manager with overall responsibility for leading and managing the entity's	6.1 INTERNAL ORGANIZATION 6.1.1 Management commitment to information security

Copyright 2012, Information Shield, Inc.

	implementation of, and adherence to, Standards CIP-002 through CIP-009.	6.1.2 Information security co-ordination 6.1.3 Allocation Of Information Security Responsibilities
R3. Exceptions	Instances where the RE cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	5.1.2 Review of the information security policy
R4. Information Protection	The RE shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	7.2 Information Classification 7.2.1 Classification Guidelines 7.2.2 Information Labeling And Handling (42 policies)
R5. Access Control	The RE shall document and implement a program for managing access to protected Critical Cyber Asset information.	11 Access Control 11.2 User Access Management 11.4 Network Access Control 11.5 Operating System Access Control 11.6 Application and Information Access Control
R6. Change Control and Configuration Management	The RE shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 10.1.1 Documented operating procedures 10.1.2 Change management 10.1.3 Segregation of duties 10.1.4 Separation of development, test, and operational facilities 10.3 SYSTEM PLANNING AND ACCEPTANCE. 10.3.1 Capacity management 10.3.2 System acceptance
CIP–004–4	**Personnel and Training**	8 HUMAN RESOURCES SECURITY
R1. Awareness	The RE shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.	8.2.2 Information security awareness, education, and training
R2. Training	The RE shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets,	8.2.2 Information security awareness, education, and training
R3. Personnel Risk Assessment	The RE shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.	8.1 PRIOR TO EMPLOYMENT 8.1.1 Roles and responsibilities 8.1.2 Screening 8.1.3 Terms and conditions of employment 8.2 DURING EMPLOYMENT 8.2.1 Management responsibilities 8.2.3 Disciplinary process
R4. Access	The RE shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	8.3.3 Removal of access rights 11.2 User Access Management 11.5.2 User identification and authentication 11.3 USER RESPONSIBILITIES 11.3.1 Password use. 11.3.2 Unattended user equipment

Copyright 2012, Information Shield, Inc.

		11.3.3 Clear desk and clear screen policy
CIP–005–4	**Electronic Security Perimeter(s)**	11.4 NETWORK ACCESS CONTROL
R1. Electronic Security Perimeter	The RE shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The RE shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	11.1.1 Access control policy
R2. Electronic Access Controls	The RE shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	11.4 NETWORK ACCESS CONTROL 11.5 OPERATING SYSTEM ACCESS CONTROL 11.6 APPLICATION AND INFORMATION ACCESS CONTROL
R3. Monitoring Electronic Access	The RE implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	10.10 MONITORING 10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging 10.10.6 Clock synchronization
R4. Cyber Vulnerability Assessment	The RE shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually.	12.6 TECHNICAL VULNERABILITY MANAGEMENT 12.6.1 Control of technical vulnerabilities
R5. Documentation Review and Maintenance	The RE shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	5.1.2 Review of the information security policy 15.2.2 Technical compliance checking
CIP-006-4	**Physical Security**	9 PHYSICAL AND ENVIRONMENTAL SECURITY
R1. Physical Security Plan	The RE shall create and maintain a physical security plan,	9.1 SECURE AREAS 9.1.1 Physical security perimeter
R2. Physical Access Controls	The RE shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week.	9.1.2 Physical entry controls 9.1.3 Securing offices, rooms, and facilities
R3. Monitoring Physical Access	The RE shall document technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week.	9.1.2 Physical entry controls
R4. Logging Physical Access	Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week.	9.1.2 Physical entry controls 10. Access Control System Records 12. Physical Access Grantor List 13. Identification Badge Reports
R5. Access Log Retention	The RE shall retain physical access logs for at least ninety calendar days.	9.1.2 Physical entry controls 10. Access Control System Records
R6. Maintenance and Testing	The RE shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.	
CIP–007–4	**Systems Security Management**	

Copyright 2012, Information Shield, Inc.

R1. Test Procedures	The RE shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls.	10.3 SYSTEM PLANNING AND ACCEPTANCE
R2. Ports and Services	The RE shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	10.6.1 Network controls
R3. Security Patch Management		12.5.2 Technical review of applications after operating system changes 12.5.3 Restrictions on changes to software packages 12.5.4 Information leakage
R4. Malicious Software Prevention		10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE
R5. Account Management	shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. **R5.2**. The RE shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts. **R5. 3** shall require and use passwords,	11.5 OPERATING SYSTEM ACCESS CONTROL 11.5.1 Secure log-on procedures 11.5.2 User identification and authentication 11.5.3 Password management system 11.5.4 Use of system utilities 11.5.5 Session time-out 11.5.6 Limitation of connection time 11.2 USER ACCESS MANAGEMENT. 11.2.1 User registration 11.2.2 Privilege management 11.2.3 User password management
R6. Security Status Monitoring	process controls to monitor system events that are related to cyber security.	10.10.2 Monitoring system use 15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS
R7. Disposal or Redeployment	The RE shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	10.7.1 Management of removable media 10.7.2 Disposal of media 10.7.3 Information handling procedures 10.7.4 Security of system documentation
R8. Cyber Vulnerability Assessment	The RE shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually.	12.6.1 Control of technical vulnerabilities
CIP–008–4	**Incident Reporting and Response Planning**	13 INFORMATION SECURITY INCIDENT MANAGEMENT
R1. Cyber Security Incident Response Plan	The RE shall develop and maintain a Cyber Security Incident response plan.	13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES 13.1.1 Reporting information security events 13.1.2 Reporting security weaknesses
R2. Cyber Security Incident Documentation	The RE shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 13.2.1 Responsibilities and procedures 13.2.2 Learning from information security incidents 13.2.3 Collection of evidence
CIP–009–4	**Recovery Plans for Critical Cyber**	14 BUSINESS CONTINUITY

Copyright 2012, Information Shield, Inc.

	Assets	MANAGEMENT
R1. Recovery Plans	The RE shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following: R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s). R1.2. Define the roles and responsibilities of responders.	14.1.1 Including information security in the business continuity management process 14.1.2 Business continuity and risk assessment 14.1.3 Developing and implementing continuity plans including information security
R2. Exercises	The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	14.1.4 Business continuity planning framework 14.1.5 Testing, maintaining and re-assessing business continuity plans
R3. Change Control	Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.	14.1.5 Testing, maintaining and re-assessing business continuity plans
R4. Backup and Restore	The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets.	10.5.1 Information back-up
R5. Testing Backup Media	Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	10.5.1 Information back-up

[1] Information based on material found in Mandatory Reliability Standards for Critical Infrastructure Protection (18 CFR Part 40 – Update 4), available from the Federal Energy Regulatory Commission (FERC). Security policy categories based on the ISO 27002 information security standard and the PolicyShield Security Policy Subscription Service.

Copyright 2012, Information Shield, Inc.