

Table of Contents

Acronyms and Abbreviations	vii
Executive Summary	1
Introduction	7
I: Get Started	11
Step 1: Build a Team and Select an Approach	11
Assemble Compliance Teams and Leadership	11
Develop a Compliance Timeline	11
Step 2: Identify Assets and Perimeters	12
Define a Risk-based Methodology to Identify Critical Cyber Assets	15
Define Electronic Security Perimeters (ESP)	21
Define a Physical Security Perimeter	26
II: Create Documentation System and Train Security Personnel	29
Step 3: Assess Documentation Requirements	29
Step 4: Train Security Management Controls Personnel	29
III: Securing Physical and Cyber Assets	31
Step 5: Assess Physical Security Readiness (CIP-006)	31
Step 6: Assess Cyber Security Readiness (CIP-005, 007)	31
Electronic Access Controls	32
Set Passwords	34
Secure Computers in Substations	35
Monitor Electronic Access	36

Implement Early Warning System.....	37
IV: Incident Reporting	39
Steps 7: Implement Incident Reporting Processes and Recovery Plans (CIP-008, 009)	39
V: Implement Compliance Technology	41
Step 8: Implement Technology to Automate Compliance Requirements	41
Step 9: Implement Processes to Collect Compliance Documentation.....	41
Create Security Data Logs and Diagnostics	41
Monitor Security Status Indications.....	42
VI: Prepare for a NERC audit.....	47
Step 10: Conduct a pre-audit assessment	47
VII. What May Change: the FERC NOPR	49
Applicability.....	49
Performance-Based Compliance	50
Language.....	50
Use of Other Standards	51
Conclusion	53
Appendix I: Summary of Key Provisions of NERC CIP Standards 002-009.	55
Appendix II: NERC CIP Standards Compliance Checklist.....	61