

# Table of Contents

<b>Acronyms and Abbreviations .....</b>	<b>vii</b>
<b>Executive Summary.....</b>	<b>1</b>
<b>Introduction.....</b>	<b>7</b>
<b>I: Get Started .....</b>	<b>11</b>
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
<b>II: Create Documentation System and Train Security Personnel .....</b>	<b>29</b>
Step 3: Assess Documentation Requirements .....	29
Step 4: Train Security Management Controls Personnel.....	29
<b>III: Securing Physical and Cyber Assets.....</b>	<b>31</b>
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
<b>IV: Incident Reporting .....</b>	<b>39</b>
Steps 7: Implement Incident Reporting Processes and Recovery Plans (CIP-008, 009) .....	39
<b>V: Implement Compliance Technology .....</b>	<b>41</b>
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
<b>VI: Prepare for a NERC audit.....</b>	<b>47</b>
Step 10: Conduct a pre-audit assessment .....	47
<b>VII. What May Change: the FERC NOPR .....</b>	<b>49</b>
Applicability.....	49
Performance-Based Compliance .....	50
Language.....	50
Use of Other Standards .....	51
<b>Conclusion .....</b>	<b>53</b>
<b>Appendix I: Summary of Key Provisions of NERC CIP Standards 002-009.</b>	<b>55</b>
<b>Appendix II: NERC CIP Standards Compliance Checklist.....</b>	<b>61</b>