Mapping NERC CIP V3 to V5, SANS Top 20 Critical Controls, and NIST 800 Series Pubs

The Anfield Group

For any feedback or suggestions on this poster, please
contact : info@theanfieldgroup.com
www.theanfieldgroup.com

NERC CIP Version 3	NERC CIP Version 5	SANS TOP 20 Critical Controls	NIST 800 Series Special Publications
CIP-002-3 Critical Cyber Asset Identification	**CIP-002-5 BES Cyber System Categorization**		NIST SP-800-53 Rev 4 "Security and Privacy Controls for Federal Information Systems and Organizations SP 800-82 Rev 2 Guide to Industrial Control System Security SP-800-27 Engineering Principles for Information Technology Security
R1: Risk-Based Assessment Methodology (RBAM) to id Critical Assets (CA)	**R1: Attachment 1 CIP-002-5 Incorporates the "Bright Line Criteria" to classify BES Assets as Low, Medium, or High. Called BES Cyber Systems consolidating CAs and CCAs**	Control 1: Inventory of Authorized and Unauthorized Devices Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation	
R2: Apply RBAM to ID Critical Assets	**R2: BES Cyber System Lists must be reviewed and approved every 15 calendar months**		
R3: Identify Critical Cyber Assets (CCA)			
R4: Annual Approval of RBAM, CA list, and CCA List			
CIP-003-3 Security Management Controls	**CIP-003-5 Security Management Controls**		NIST SP-800-53 Rev 4 "Security and Privacy Controls for Federal Information Systems and Organizations NIST SP-800-100 Information Security Handbook: A Guide For Managers
R1: Cyber Security Policy	R1: Cyber Security Policies approved for Medium and High Impact BES Cyber Systems by CIP Senior Manager every 15 calendar months. Cyber Security Policies for Medium and High Impact BES Cyber Systems must address CIP-004-CIP-011 (CIP-010 Configuration Change Management and Vulnerability Assessments, CIP-011 Information Protection) as well as Declaring and Responding to CIP Exceptional Circumstances	Critical Control 15: Controlled Access based on need to know Critical Control 3: Secure Configurations for hardware and software on mobile devices,laptops, workstations, and servers Critical Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Critical Control 18: Incident Response and Management	
R2: CIP Senior Manager Identification	R2: Cyber Security Policies approved for Low Impact Assets by CIP Senior Manager every 15 Calendar Months. Cyber Security Policies for low impact assets must include Cyber Security Awareness, Physical Security Controls, Electronic Access Controls for external routable protocol connections and dial-up connectivity and incident response to Cyber Security Incident. **An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required**	Critical Control 15: Controlled Access based on need to know Critical Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches Critical Control 18: Incident Response and Management Critical Control 13: Boundary Defense	
R3: Exceptions to the Cyber Security Policy	R3: Identify a CIP Senior Manager and document any change within 30 calendar days of the change		
R4: Information Protection Program	R4: CIP Senior Manager must document any delegates		
R5: Access Control			
R6: Change Control and Configuration Management			
CIP-004-3 Personnel and Training	**CIP-004-5 Personnel and Training**		SP800-50 Building an Information Technology Security and Awareness Program SP-800-89 Recommendation for Obtaining Assurances for Digital Signature Applications
R1: Awareness: Security Awareness Program	R1: Security Awareness Program- reference Table 1: Security Awareness Program Criteria in standard	Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps	
R2: Training: Cyber Security Training Program	R2: Training Program- reference Table R2 Cyber Security Training Program in standard	Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps	
R3: Personnel Risk Assessment	R3: PRA Program- reference Table R3 PRA Program in standard	Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps	
R4: Access	R4: Access Management Program- Reference Table R4 Access Management Program in standard for required program criteria	Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps	
	R5: Access Revocation Program- Reference Table R5 Access Revocation for required program criteria	Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps	
CIP-005-3 Electronic Security Perimeter(s)	**CIP-005-5 Electronic Security Perimeter(s)**		SP-800-162 Guide to Attribute Based Access Control Definition and Considerations SP-800-125 Guide to Security for full Virtualization Technologies SP-800-125 A: DRAFT Security Recommendations for Hypervisor Deployment SP-800-41 Guidelines on Firewalls and Firewall Policies SP-800-42 Guidelines on Network Security Testing SP-800-63 Electronic Authentication Guideline SP-800-120 Recommendation for EAP Methods Used in Wireless Network Access Authentication
R1: Electronic Security Perimeters: All CCAs must reside within an ESP	R1: Electronic Security Perimeters- reference Table R1 Electronic Security Perimeter for required criteria	Control 1: Inventory of Authorized and Unauthorized Devices Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 13: Boundary Defense	
R2: Electronic Access Controls	R2: Interactive Remote Access Management Table R2	Control 1: Inventory of Authorized and Unauthorized Devices Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 13: Boundary Defense Critical Control 16: Account Monitoring and Control	
R3: Monitoring Electronic Access		Control 1: Inventory of Authorized and Unauthorized Devices Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 13: Boundary Defense Critical Control 16: Account Monitoring and Control	
R4: Cyber Vulnerability Assessment		Control 1: Inventory of Authorized and Unauthorized Devices Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 13: Boundary Defense Critical Control 16: Account Monitoring and Control	
R5: Documentation Review and Maintenance		Control 1: Inventory of Authorized and Unauthorized Devices Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation Critical Control 13: Boundary Defense Critical Control 16: Account Monitoring and Control	
CIP-006-3 Physical Security	**CIP-006-5 Physical Security of BES Cyber Systems**		SP-800-30 Guide for Conducting Risk Assessments SP-800-53 Physical and Environmental Protection SP-800-137 Information Security and Continuous Monitoring
R1: Physical Security Plan	R1: Physical Security Plan table for criteria	Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense	
R2: Protection of Physical Access Control Systems	R2: Visitor Control Plan- see table R2 Visitor Control Plan for criteria	Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense	
R3: Protection of Electronic Access Control Systems	R3: Maintenance and Testing Program see table R3	Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense	
R4: Physical Access Controls		Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense	
R5: Monitoring Physical Access		Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense Critical Control 14: Maintenance, Monitoring and Analysis of Audit Logs	
R6: Logging Physical Access		Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense Critical Control 14: Maintenance, Monitoring and Analysis of Audit Logs	
R7: Access Log Retention		Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense Critical Control 14: Maintenance, Monitoring and Analysis of Audit Logs	
R8: Maintenance and Testing		Critical Control 9: Security Skills Assessment and Appropriate Training to fill gaps Critical Control 15: Controlled Access based on need to know Critical Control 13: Boundary Defense Critical Control 14: Maintenance, Monitoring and Analysis of Audit Logs	
CIP-007-3 Systems Security Management	**CIP-007-5 Systems Security Management**		SP-800-162 Guide to Attribute Based Access Control Definition and Considerations SP-800-125 Guide to Security for full Virtualization Technologies SP-800-125 A: DRAFT Security Recommendations for Hypervisor Deployment SP-800-41 Guidelines on Firewalls and Firewall Policies SP-800-42 Guidelines on Network Security Testing SP-800-53 Security and Privacy Controls for Federal Information Systems and Organizations SP-800-64 Security Considerations in the System Development Life cycle SP-800-81-2 Secure Domain Name System Deployment Guide SP-800-85-B PIV Data Model Conformance Test Guidelines SP-800-92 Guide to Computer Security Log Management SP-800-94 Guide to Intrusion Detection and Prevention Systems SP-800-95 Guide to Secure Web Services SP-800-114 User's Guide to Securing External Devices for Telework and Remote Access SP-800-115 Technical Guide to Information Security Testing and Assessments SP-800-118 Guide to Enterprise Password Management SP-800-123 Guide to General Server Security SP-800-30 Guide for Conducting Risk Assessments SP-800-40 Guide to Enterprise Patch Management Technologies SP-800-167 Guide to Application Whitelisting
R1: Test Procedures	R1: Ports and Services See Table 1: Ports and Services in the standard for required criteria	Critical Control 13: Boundary Defense Critical Control 6: Application Software Security Critical Control 10: Secure Configurations for Network Devices such as Firewalls, routers and switches Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	
R2: Ports and Services	R2: Security Patch Management Table R2 for required criteria	Critical Control 13: Boundary Defense Critical Control 6: Application Software Security Critical Control 10: Secure Configurations for Network Devices such as Firewalls, routers and swi tches Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	
R3: Security Patch Management	R3: Malicious Code Prevention. See table R3 for required criteria	Critical Control 4: Continuous Vulnerability Assessment and remediation Critical Control 5: Malware Defenses Critical 6: Application Software Security Critical Control 20: Penetration Tests and Red Teaming	
R4: Malicious Software Prevention	R4: Security Event Monitoring. See table R4 for required criteria	Critical Control 16: Account Monitoring and Control Critical Control 18: Incident Response and Management Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	
R5: Account Management	R5: System Access Controls. See table R5 for required criteria	Critical Control 15: Controlled Access based on need to know Critical Control 19: Secure Network Engineering Critical Control 16: Account Monitoring and Control	
R6: Security Status Monitoring		Critical Control 16: Account Monitoring and Control Critical Control 18: Incident Response and Management Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs	
R7: Disposal or Redeployment		Critical Control 8: Data Recovery Capability	
R8: Cyber Vulnerability Assessment		Critical Control 4: Continuous Vulnerability Assessment and Remediation	
R9: Documentation Review and Maintenance			
CIP-008-3 Incident Reporting and Response Planning	**CIP-008-5 Incident Reporting and Response Planning**		SP-800-53 Security and Privacy Controls for Federal Information Systems and Organizations SP-800-39 Managing Information Security Risk: Organization, Mission, and Information System View SP-800-34 Contingency Planning Guide for Federal Information Systems SP-800-61-2 Computer Security Incident Handling Guide SP-800-83 Guide to Malware Incident Prevention and Handling for Laptops and Desktops
R1: Cyber Security Incident Response Plan	R1: Cyber Security Incident Response Plan	Critical Control 18: Incident Response and Management	
R2: Cyber Security Incident Documentation	R2: Implementation and testing of Cyber Security Incident Response Plans	Critical Control 18: Incident Response and Management	
	R3: Cyber Security Incident Response Plan Review, Update and Communication	Critical Control 18: Incident Response and Management	
CIP-009-3 Recovery Plans for Critical Cyber Assets	**CIP-009-5 Recovery Plans for BES Cyber Systems**		SP-800-34 Contingency Planning Guide for Federal Information Systems SP-800-53 Security and Privacy Controls for Federal Information Systems and Organizations SP-800-18 Guide for Developing Security Plans for Federal Information Systems SP-800-88 Guidelines for Media Sanitization
R1: Recovery Plans	Recovery Plan Specifications see table R1	Critical Control 17: Data Loss Prevention Critical Control 18: Incident Response and Management Critical Control 8: Data Recovery Capability	
R2: Exercises	Recovery Plan Implementation and Testing see table R2	Critical Control 17: Data Loss Prevention Critical Control 18: Incident Response and Management Critical Control 8: Data Recovery Capability	
R3: Change Control	Recovery Plan review, udpate and communication	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
R4: Backup and Restore		Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
R5: Testing Back Up Media		Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
	CIP-010-1 Configuration Change Management and Vulnerability Assessments	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	SP-800-53 Security and Privacy Controls for Federal Information Systems and Organizations SP-800-167 Guide to Application Whitelisting SP-800-150 Guide to Cyber Threat Information Sharing SP-800-142 Practicing Combinatorial Testing SP-800-128 Guide for Security-Focused Configuration Management of Information Systems SP-800-115 Technical Guide to Information Security Testing and Assessments SP-800--39 Managing Information Security Risk: Organization, Mission, and Information System View
	R1: Configuration Change Management Process see table R1	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
	R2: Configuration Monitoring see table R2	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
	R3: Vulnerability Assessments Table R3	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
	CIP-011-1 Information Protection	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	SP-800-53 Security and Privacy Controls for Federal Information Systems and Organizations SP-800-168 Approximate Matching: Definition and Terminology SP-800-150 Guide To Cyber Threat Information Sharing SP-800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations SP-800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information SP-800-115 Technical Guide to Information Security Testing and Assessment SP-800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
	R1: Information Protection Process- see table R1	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	
	R2: BES Cyber Asset Reuse and Disposal	Critical Control 1: Inventory of Authorized and Unauthorized devices Critical Control 2: Inventory of Authorized and Unauthorized Software Critical Control 8: Data Recovery Capability	