NERC CIP Standard Mapping to the Critical Security Controls - Draft

For any feedback or suggestions on this poster, please contact :

CIP@securingthehuman.org
www.securingthehuman.org/utility

NERC CIP Version 3	NERC CIP Version 4	NERC CIP Version 5	Critical Security Controls
CIP-002-3 Critical Cyber Asset Identification	**CIP-002-4 Critical Cyber Asset Identification**	**CIP-002-5 BES Cyber System Categorization**	
R1: Risk-Based Assessment Methodology (RBAM) to id Critical Assets (CA)	Attachment 1: Critical Asset Criteria added to determine criticality. No more RBAM. Sub-requirements R1.1 and R1.2 now N/A	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 Device Control 2: Inventory of Authorized and Unauthorized Software Control 4: Continuous Vulnerability Assessment and Remediation
R2: Apply RBAM to ID Critical Assets	N/A	R2: BES Cyber System Lists must be reviewed and approved every 15 calendar months	
R3: Identify Critical Cyber Assets (CCA)	Now R2		
R4: Annual Approval of RBAM, CA list, and CCA List	Now R3		
CIP-003-3 Security Management Controls	**CIP-003-4 Security Management Controls**	**CIP-003-5 Security Management Controls**	
R1: Cyber Security Policy	No Change	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	No Change	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 reponse to Cyber Security Incident. An inventory, list, or descrete 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	No Change	R3: Identify a CIP Senior Manager and document any change within 30 calendar days of the change	
R4: Information Protection Program	No Change	R4: CIP Senior Manager must document any delegates	
R5: Access Control	No Change		
R6: Change Control and Configuration Management	No Change		
CIP-004-3 Personnel and Training	**CIP-004-4 Personnel and Training**	**CIP-004-5 Personnel and Training**	
R1: Awareness: Security Awareness Program	No Change	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	No Change	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	No Change	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	No Change	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-005-4 Electronic Security Perimeter(s)**	**CIP-005-5 Electronic Security Perimeter(s)**	
R1: Electronic Security Perimeters: All CCAs must reside within an ESP	No Change	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	No Change	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	No Change		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	No Change		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	No Change		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-006-4 Physical Security**	**CIP-006-5 Physical Security of BES Cyber Systems**	
R1: Physical Security Plan	No Change	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	No Change	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	No Change	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	No Change		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	No Change		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 Analyis of Audit Logs
R6: Logging Physical Access	No Change		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 Analyis of Audit Logs
R7: Access Log Retention	No Change		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 Analyis of Audit Logs
R8: Maintenance and Testing	No Change		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 Analyis of Audit Logs
CIP-007-3 Systems Security Management	**CIP-007-4 Systems Security Management**	**CIP-007-5 Systems Security Management**	
R1: Test Procedures	No Change	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	No Change	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 switches Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
R3: Security Patch Management	No Change	R3: Malicious Code Prevention. See table R3 for required criteria	Critical Control 4: Continuous Vulnerabilty 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	No Change	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	No Change	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	No Change		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	No Change		Critical Control 8: Data Recovery Capability
R8: Cyber Vulnerabiliity Assessment	No Change		Critical Control 4: Continuous Vulnerability Assessment and Remediation
R9: Documentation Review and Maintenance	No Change		
CIP-008-3 Incident Reporting and Response Planning	**CIP-008-4 Incident Reporting and Response Planning**	**CIP-008-5 Incident Reporting and Response Planning**	
R1: Cyber Security Incident Response Plan	No Change	R1: Cyber Security Incident Response Plan	Critical Control 18: Incident Response and Management
R2: Cyber Security Incident Documentation	No Change	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-009-4 Recovery Plans for Critical Cyber Assets**	**CIP-009-5 Recovery Plans for BES Cyber Systems**	
R1: Recovery Plans	No Change	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	No Change	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	No Change	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	No Change		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	No Change		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
		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
		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