National CyberWatch Center – Cybersecurity Foundation Series Curriculum Standards

Working Group Topic Areas

Based on Function Definitions and Categories from the
Framework for Improving Critical Infrastructure Cybersecurity (aka "Cybersecurity Framework")

NOTE: All of the following functions, categories, and definitions are all taken directly from the NIST Cybersecurity Framework, including the cross-reference mapping to standard controls identified within SP-800-53, Rev. 4, Appendix F (Security Control Catalog) and Appendix J (Privacy Control Catalog). Abbreviations for the NIST control families have the following meanings:

Abbrev	Definition	Abbrev	Definition
Security Control Families			
AC	Access Control	AT	Awareness and Training
AU	Audit and Accountability	CA	Security Assessment and Authorization
CM	Configuration Management	CP	Contingency Planning
IA	Identification and Authentication	IR	Incident Response
MA	Maintenance	MP	Media Protection
PE	Physical and Environmental Protection	PL	Planning
PS	Personnel Safety	RA	Risk Assessment
SA	System and Services Acquisition	SC	System and Communications Protection
SI	System and Information Integrity		
Privacy Control Families			
AP	Authority and Purpose	AR	Accountability, Audit, and Risk Management
DI	Data Quality and Integrity	DM	Data Minimization and Retention
IP	Individual Participation and Redress	SE	Security
TR	Transparency	UL	Use Limitation

Topic Area #1 – "Identify"

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of **outcome Categories within this Function include:** Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

This function and its categories and subcategories have been mapped to the following controls from NIST SP-800-53, Rev. 4; Appendix D, Table D-2; and Appendix G, Table G-1:

Control	Control Name	Control	Control Name
AC-20	Use of External Information Systems	PM-15	Contacts with Security Groups and Associations
AC-4	Information Flow Enforcement	PM-16	Threat Awareness Program
CA-2	Security Assessments	PM-4	Plan of Action and Milestones Process
CA-3	System Interconnections	PM-8	Critical Infrastructure Plan
CA-7	Continuous Monitoring	PM-9	Risk Management Strategy
CA-8	Penetration Testing	PS-7	Third-Party Personnel Security
CA-9	Internal System Connections	RA-2	Security Categorization
CM-8	Information System Component Inventory	RA-3	Risk Assessment
CP-11	Alternate Communications Protocols	RA-5	Vulnerability Scanning
CP-2	Contingency Plan	SA-11	Developer Security Testing and Evaluation
CP-8	Telecommunications Services	SA-12	Supply Chain Protection
PE-11	Emergency Power	SA-14	Criticality Analysis
PE-9	Power Equipment and Cabling	SA-5	Information System Documentation
PL-8	Information Security Architecture	SA-9	External Information System Services
PM-1	Information Security Program Plan	SI-2	Flaw Remediation
PM-11	Mission/Business Process Definition	SI-4	Information System Monitoring
PM-12	Insider Threat Program	SI-5	Security Alerts, Advisories, and Directives

~ ~ End of Table ~ ~

<u>Topic Area #2</u> – "Protect/Detect"

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of **outcome Categories within this Function include:** Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

The Detect Function enables timely discovery of cybersecurity events. Examples of **outcome Categories within this Function include:** Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

This function and its categories and subcategories have been mapped to the following controls from NIST SP-800-53, Rev. 4; Appendix D, Table D-2; and Appendix G, Table G-1:

Control	Control Name	Control	Control Name
AC-16	Security Attributes	MP-7	Media Use
AC-17	Remote Access	PE-10	Emergency Shutoff
AC-18	Wireless Access	PE-12	Emergency Lighting
AC-19	Wireless Access	PE-13	Fire Protection
AC-2	Account Management	PE-14	Temperature and Humidity Controls
AC-20	Use of External Information Systems	PE-15	Water Damage Protection
AC-21	Information Sharing	PE-16	Delivery and Removal
AC-3	Access Enforcement	PE-18	Location of Information System Components
AC-4	Information Flow Enforcement	PE-19	Information Leakage
AC-5	Separation of Duties	PE-2	Physical Access Authorizations
AC-6	Least Privilege	PE-20	Asset Monitoring and Tracking
AT-2	Security Awareness Training	PE-3	Physical Access Control
AT-3	Role-Based Security Training	PE-4	Access Control for Transmission Medium
AU Family	Audit and Accountability	PE-5	Access Control for Output Devices
AU-12	Audit Generation	PE-6	Monitoring Physical Access
AU-13	Monitoring for Information Disclosure	PE-9	Power Equipment and Cabling
AU-4	Audit Storage Capacity	PL-2	System Security Plan

Control	Control Name	Control	Control Name
AU-6	Audit Review, Analysis, and Reporting	PL-8	Information Security Architecture
CA-2	Security Assessments	PM-13	Information Security Workforce
CA-3	System Interconnections	PM-14	Testing, Training, and Monitoring
CA-7	Continuous Monitoring	PM-6	Information Security Measures of Performance
CM-10	Software Usage Restrictions	PS Family	Personnel Safety
CM-11	User-Installed Software	PS-3	Personnel Screening
CM-2	Baseline Configuration	PS-6	Access Agreements
CM-3	Configuration Change Control	PS-7	Third-Party Personnel Security
CM-4	Security Impact Analysis	RA-3	Risk Assessment
CM-5	Access Restrictions for Change	RA-5	Vulnerability Scanning
CM-6	Configuration Settings	SA-10	Developer Configuration Management
CM-7	Least Functionality	SA-11	Developer Security Testing and Evaluation
CM-8	Information System Component Inventory	SA-12	Supply Chain Protection
CM-9	Configuration Management Plan	SA-15	Development Process, Standards, and Tools
CP-2	Contingency Plan	SA-17	Developer Security Architecture and Design
CP-4	Contingency Plan Testing	SA-3	System Development Life Cycle
CP-6	Alternate Storage Site	SA-4	Acquisition Process
CP-8	Telecommunications Services	SA-8	Security Engineering Principles
CP-9	Information System Backup	SA-9	External Information System Services
IA Family	Identification and Authentication	SC-13	Cryptographic Protection
IR-3	Incident Response Testing	SC-18	Mobile Code
IR-4	Incident Handling	SC-28	Protection of Information at Rest
IR-5	Incident Monitoring	SC-31	Covert Channel Analysis
IR-8	Incident Response Plan	SC-44	Detonation Chambers
MA-2	Controlled Maintenance	SC-5	Denial of Service Protection
MA-3	Maintenance Tools	SC-7	Boundary Protection
MA-4	Nonlocal Maintenance	SC-8	Transmission Confidentiality and Integrity

Control	Control Name	Control	Control Name
MA-5	Maintenance Personnel	SI-2	Flaw Remediation
MP-2	Media Access	SI-3	Malicious Code Protection
MP-4	Media Storage	SI-4	Information System Monitoring
MP-5	Media Transport	SI-7	Software, Firmware, and Information Integrity
MP-6	Media Sanitization		

~ ~ End of Table ~ ~

<u>Topic Area #3</u> – "Respond/Recover"

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of **outcome Categories within this Function include:** Response Planning; Communications; Analysis; Mitigation; and Improvements.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of **outcome Categories within this Function include:** Recovery Planning; Improvements; and Communications.

This function and its categories and subcategories have been mapped to the following controls from NIST SP-800-53, Rev. 4; Appendix D, Table D-2; and Appendix G, Table G-1:

Control	Control Name	Control	Control Name
AU-6	Audit Review, Analysis, and Reporting	IR-6	Incident Reporting
CA-2	Security Assessments	IR-8	Incident Response Plan
CA-7	Continuous Monitoring	PE-6	Monitoring Physical Access
CP-10	Information System Recovery and Reconstitution	PM-15	Contacts with Security Groups and Associations
CP-2	Contingency Plan	RA-3	Risk Assessment
CP-3	Contingency Training	RA-5	Vulnerability Scanning
IR-3	Incident Response Testing	SI-4	Acquisition Process
IR-4	Incident Handling	SI-5	Information System Documentation
IR-5	Incident Monitoring		

~ ~ End of Table ~ ~