National CyberWatch Center – Cybersecurity Foundation Series Curriculum Standards

Working Group Topic Areas

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

The following list of Categories within each Function can be used for the Week 1 Activity in mapping Learning Objectives and Knowledge Units to each Category.

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. These Categories are defined as follows:

Asset Management: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business Environment: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Topic Area #2 – "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. These Categories are defined as follows:

Access Control: Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Awareness and Training: The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Maintenance: Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

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. These Categories are defined as follows:

Anomalies and Events: Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security Continuous Monitoring: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes: Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Topic Area #3 – "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. These Categories are defined as follows:

Response Planning: Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Communications: Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis: Analysis is conducted to ensure adequate response and support recovery activities.

Mitigation: Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

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. These Categories as defined as follows:

Recovery Planning: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Improvements: Recovery planning and processes are improved by incorporating lessons learned into future activities.

Communications: Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.