Electricity Subsector Cybersecurity Risk Management Maturity Initiative

WORKING DRAFT MODEL Version 0.2b

05 April 2012

This working draft will be superseded by the release of the next draft version.

NON-PUBLIC UNTIL RELEASE | DO NOT DISCLOSE

1 Introduction

This document is a working draft of the maturity model being developed for the Electric Sector Cybersecurity Risk Management Maturity Initiative. This working draft is intended for review and discussion use only.

2 About the Initiative

The Electricity Sector Cybersecurity Risk Management Maturity Project is a White House initiative to develop a common risk-based model to measure cybersecurity capabilities within the electricity sector. The model is designed to help the electric sector evaluate their cybersecurity capabilities in a consistent manner, communicate capability levels in meaningful terms, and guide an organization in prioritizing cybersecurity investments.

The ESCRMM initiative is being led by the Department of Energy (DOE) in partnership with the Department of Homeland Security (DHS) and in collaboration with industry and government representatives. The initiative is an important step toward an objective, holistic way to address the electricity sector's cybersecurity risks with an appropriate balance of protection, resilience, and restoration. The initiative brings together existing cybersecurity resources and aligns them with sector-specific and cross-sector cybersecurity strategies. When complete, the initiative will allow both industry and government leaders to better understand the capabilities of the sector to manage cybersecurity risks. The model is developed as a common model that can be used by the various types of entities operating within the sector, including investor-owned, municipal, and cooperative utilities. It will also enable utilities to communicate cybersecurity capabilities in meaningful terms and prioritize their cybersecurity actions and investments.

3 Model Structure

The model structure includes domains—logical groupings of cybersecurity risk management activities—and maturity indicator levels (MILs). The content within each domain includes characteristics, which are expressions of domain activities at each level of maturity.

3.1 Domains

The model includes 10 domains, or logical groupings of cybersecurity risk management activities. Each domain is described by a title, such as "Identity and Access Management," and a shorthand reference appearing in all caps, such as "ACCESS."

A description of the each domain is provided to describe the domain in the context of this model. With the exception of the *Risk Management* domain, each domain descriptions includes the phrase "commensurate with the risk to critical infrastructure and organization objectives" to clarify that domain activities are based on the organization's risk strategy.

1. **Asset, Change, and Configuration Management (ASSET)**
   Manage the organization's operational technology (OT) and information technology (IT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives, including activities to:

- Identify, inventory, and prioritize assets,
- Manage asset configurations, and
- Manage changes to assets and to the asset inventory.

2. **Workforce Management (WORKFORCE)**
   Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

3. **Identity and Access Management (ACCESS)**
   Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

4. **Risk Management (RISK)**
   Establish, operate, and maintain a cybersecurity risk management and mitigation program to identify and manage cybersecurity risk to the organization and its related interconnected infrastructure and stakeholders.

5. **Supply Chain and External Dependencies Management (DEPENDENCIES)**
   Establish and maintain controls to manage the cybersecurity risk associated with services and assets that are dependent on external entities, commensurate with the organization's business and security objectives.

6. **Threat and Vulnerability Management (THREAT)**
   Establish and maintain plans, procedures, and technologies to identify, analyze, and manage cybersecurity threats and vulnerabilities, commensurate with the risk to critical infrastructure and organizational objectives.

7. **Event and Incident Response, Continuity of Operations (RESPONSE)**
   Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity incidents and to sustain critical functions throughout a cyber event, commensurate with the risk to critical infrastructure and organizational objectives.

8. **Situational Awareness (SITUATION)**
   Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives.

9. **Information Sharing and Communications (SHARING)**
   Establish and maintain relationships with internal and external entities to share information, including threats and vulnerabilities, in order to reduce risks and increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

10. **Cybersecurity Program Management (CYBER)**
    Establish and maintain a cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure.

3.2 Maturity Indicator Levels

The model currently defines four maturity indicator levels (MILs), and holds a fifth level in reserve for use in future versions of the model. Each of the four defined levels is referenced by a number (0 through 3) and a name, for example, "MIL3: Managed."

MIL0 through MIL3 define the maturity progression in the model. Each level describes the approach and institutionalization of the practices in a domain at that MIL. At MIL3, there is an expectation that the activities in a domain include a strong connection to or coordination with risk management activities.

- **The maturity indicator levels apply independently to each domain**. As a result there is the potential for different MIL ratings for the 10 domains. For example, an organization could be functioning at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
- **The levels are cumulative; an organization must satisfy each of the characteristics in a level and the predecessor level(s).** For example, each of the characteristics in MIL1 and MIL2 must be satisfied for a domain in order to be rated MIL2 in the domain. Similarly, characteristics in MIL1, MIL2, and MIL3 must be satisfied in order to be rated MIL3.

3.2.1 Institutionalization Progression

The progression of institutionalization is described for each domain by a set of common characteristics. The common characteristics are summarized and description of each MIL in the sections below.

The common characteristics describe activities that are performed for each domain in the model to institutionalize the activities in that domain. Institutionalization describes the extent to which a practice or activity is ingrained into the way an organization operates. The more an activity becomes part of how an organization operates; the more likely it is that the activity will continue to be performed over time.

The maturity indicator levels define the rows in the matrix view of the model. The characteristics at the intersection of a row (MIL) and a column (domain) include expressions of the common characteristics for that level in the context of that domain. For example, MIL3 includes the common characteristic, "Personnel performing the practice have adequate skills and knowledge." In the ASSET domain, this common characteristic is expressed as, "Personnel performing ASSET activities have the skills and knowledge needed to perform their assigned responsibilities." The following table illustrates this connection between the 5th common characteristic at MIL3 and specific characteristic 7b at MIL3 in the ASSET domain.

	Common Characteristics	Specific Characteristics for the ASSET domain
MIL0		
MIL1	…	
MIL2	…	
MIL3	… 5. Personnel performing the practice have adequate skills and knowledge …	… 7. Personnel a. … b. Personnel performing ASSET activities have the skills and knowledge needed to perform their assigned responsibilities …

Table 8.2.1, Example relationship between common characteristics and specific characteristics in the ASSET domain

3.2.2 Approach Progression

The progression of approach in the model is described by the specific characteristics in a domain. "Approach" describes the completeness, thoroughness, or level of development of an activity in a domain. As an organization progresses from one MIL to the next, the organization will have more complete or more advanced implementations of the core activities in the domain. Because only the initial set of activities for a domain is expected at MIL1, the organization is also expected to be performing additional activities at higher levels consistent with their risk strategy.

The following table provides an example of the progression of approach in the ASSET domain. At MIL1, an asset inventory is available for both OT (operational technology) and IT (information technology) assets that are considered important to the function (generation, transmission, distribution, markets, or retail). The asset inventory characteristics at MIL3 call for the inventory to be complete for defined categories of assets, for those categories of assets to be selected based on a risk analysis, and for the prioritization of the assets in the inventory to be informed by risk analysis. The inventory approach at MIL3 is more compete and more advanced than at MIL1. Additionally, the connection to risk management activities is evident in the MIL3 characteristics.

	Specific Characteristics for the ASSET domain
MIL0	
MIL1	1. Asset inventory a. There is an inventory of OT (operational technology) and IT (information technology) assets that are important to the delivery of the function …
MIL2	…
MIL3	1. Asset inventory a. The asset inventory is current and complete for assets of defined categories that are selected based on risk analysis b. Asset prioritization is informed by risk analysis …

Table 8.2.2, Example progress of specific characteristics in the ASSET domain

3.2.3 Maturity Indicator Levels

MIL0: Incomplete

The model contains no common or specific characteristics for MIL 0. Performance at MIL0 simply means that MIL1 in a given domain has not been achieved.

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

In each domain, MIL 1 contains a set of specific characteristics that represent the initial set of activities within that domain. These initial activities may be performed in an ad hoc manner, but they are at least being carried out. If an organization were to start with no capability in managing cybersecurity, it should focus initially on developing the practices in the model at MIL1. There is only one common characteristic at MIL1.

MIL2: Performed	*1. Practices are performed according to a documented plan* *2. Stakeholders of the practice are identified and involved* *3. Standards and/or guidelines have been identified to guide the implementation of the practices*

Three common characteristics are present at MIL2, which represent an initial level of institutionalization of the activities in a domain:

1. The practices in the domain are being performed according to a documented plan. The focus here should be on planning to ensure that the practices are intentionally designed (or selected) to serve the organization.
2. Stakeholders for the practices are identified and involved in the performance of the practice. This could include stakeholders from within the function, from across the organization, or from outside the organization, depending on how the organization has implemented or approached an activity.
3. The organization has identified some standards and/or guidelines to inform the implementation of practices in the domain. These may simply be the reference sources the organization consulted when developing the plan for performing the practices.

The practices at MIL2 are more complete and no longer ad hoc in their implementation. As a result, the organization can be more confident that the performance of the practices will be sustained over time. Some of the specific characteristics at MIL2 lay the groundwork for strong connections across the model with Risk Management at MIL3.

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

At MIL 3, the activities in a domain have been further institutionalized and are now being managed. Seven common characteristics support this progression:

1. Managed activities in a domain receive guidance from the organization in the form of policies and governance. Policies are an extension of the planning activities that are in place at MIL2.
2. The domain activities are periodically reviewed to ensure that they conform to policy. In other words, the policies are followed to ensure that the practices continue to be performed.
3. Resources, including people, funding and tools are provided to support the domain activities.
4. Personnel are assigned responsibility and authority for performing the domain activities.
5. The personnel assigned to perform the activities have adequate domain-specific skills and knowledge to perform their assignments.
6. The activities in a domain will produce work outputs of various forms, it is important that these work outputs or ‘domain artifacts’ be controlled to ensure that the correct and current version of an artifact is available when needed and to ensure that the availability, integrity, and confidentiality of the artifacts are protected as appropriate.
7. At MIL2, the organization identifies standards and guidelines to inform the domain activities. At MIL3, the expectation is that compliance with selected standards will be included in policy and confirmed with periodic reviews. For organizations that have mandatory compliance obligations (e.g., NERC CIP), reviews to compliance with those obligations are included here.

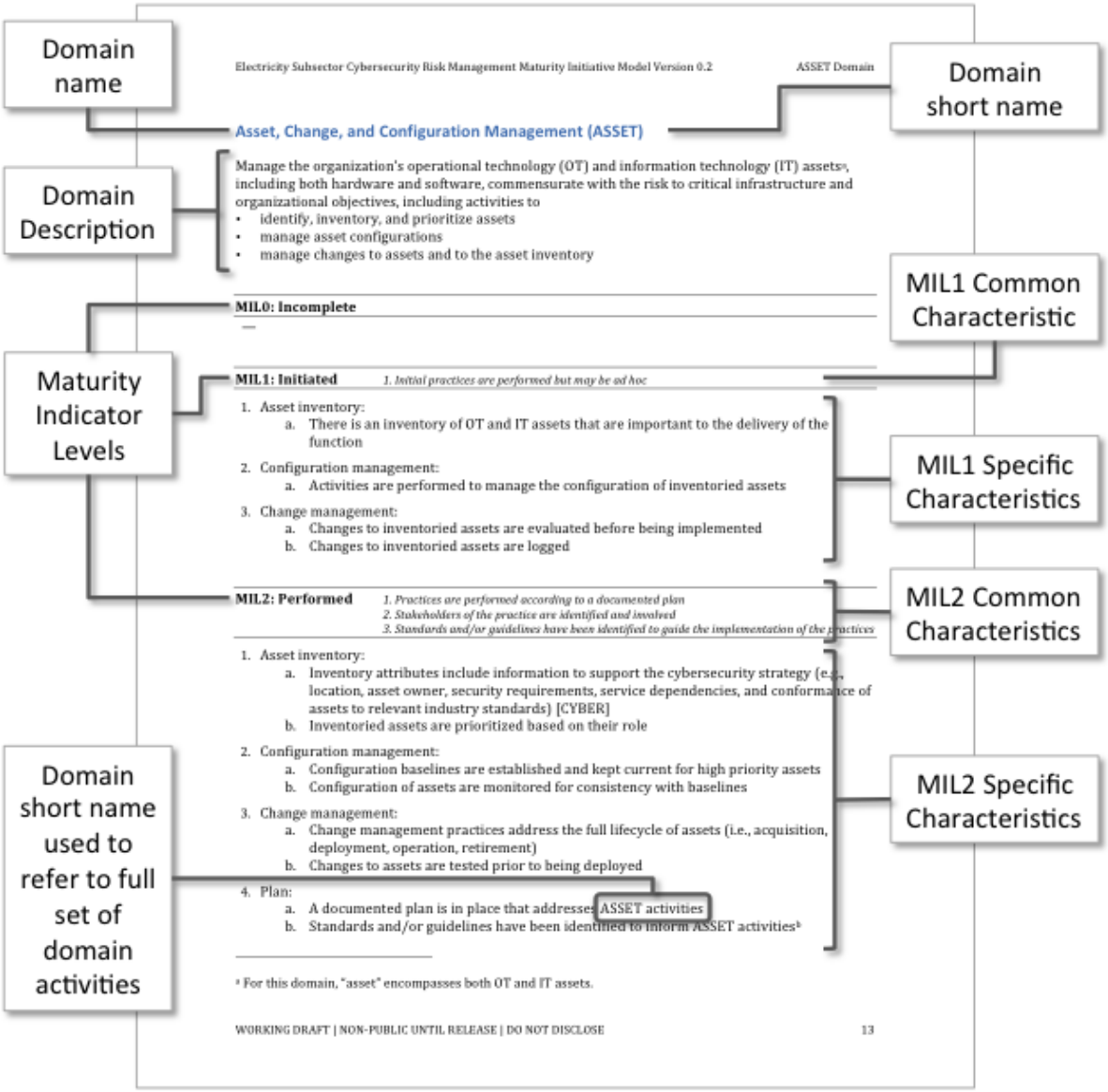
In the specific characteristics at MIL3, there is also a focus on collaboration and coordination with the Risk Management domain (RISK). This strong connection to RISK helps to scale the model to organizations of various risk profiles. Some utilities have much greater risk exposures than others. By linking the implementation of the activities at MIL3 to RISK, the activities should scale to the serve utilities at both ends of the risk exposure continuum.

MILX: Reserved for future use

During the pilot period and beyond, the model team will look for characteristics of utilities that are clearly operating above MIL3 with the expectation that they will be codified as MIL X in future versions of the model.

4 The Model

The following pages present the model domains. Each domain is presented in the same format, as shown in the figure below, which labels the various domain elements.



Asset, Change, and Configuration Management (ASSET)

Manage the organization's operational technology (OT) assets, information technology (IT) assets[a], and communication devices, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives, including activities to

- identify, inventory, and prioritize assets
- manage asset configurations
- manage changes to assets and to the asset inventory

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Asset inventory
    a. There is an inventory of OT and IT assets that are important to the delivery of the function
2. Configuration management
    a. Selected assets are controlled to ensure they remain in a common configuration (configuration management applies in cases where it is desirable to ensure that multiple assets are configured similarly)
3. Change management
    a. Changes to inventoried assets are evaluated before being implemented
    b. Changes to inventoried assets are logged

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Asset inventory
    a. Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, security requirements, service dependencies, and conformance of assets to relevant industry standards) [CYBER]
    b. Inventoried assets are prioritized based on their role
2. Configuration management
    a. Configuration baselines are established and kept current for high priority assets
    b. Configuration of assets are monitored for consistency with baselines
3. Change management
    a. Change management practices address the full lifecycle of assets (i.e., acquisition, deployment, operation, retirement)
    b. Changes to assets are tested prior to being deployed

[a] For this domain, "asset" encompasses both OT and IT assets.

4. Plan
    a. A documented plan is in place that addresses ASSET activities
    b. Standards and/or guidelines have been identified to inform ASSET activities[b]
5. Stakeholders:
    a. Stakeholders for ASSET activities are identified and involved[c]

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Asset inventory
    a. The asset inventory is current and complete for assets of defined categories that are selected based on risk analysis [RISK]
    b. Asset prioritization is informed by risk analysis [RISK]
2. Configuration management
    a. Configuration baselines are designed to satisfy cybersecurity objectives [CYBER]
    b. Modifications to configuration baselines are subject to defined change management policies
3. Change management
    a. Changes to assets are tested for cybersecurity impact prior to being deployed
    b. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)
4. Cross-domain coordination
    a. Asset inventory attributes support analysis of THREAT (i.e., inventory includes sufficient information about the assets to enable threat and vulnerability analysis)
    b. Configuration management is coordinated with cybersecurity patch management [THREAT]
    c. Change management is coordinated with THREAT activities
    d. ASSET activities are coordinated with DEPENDENCIES activities for high priority assets that are dependent on external parties
5. Policy
    a. ASSET activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines.
    c. ASSET activities are periodically reviewed to ensure conformance with policy
6. Resources
    a. Adequate resources (people, funding, and tools) are provided to support ASSET activities [CYBER]

[b] Examples of standards that address asset inventory issues include Organization for the Advancement of Structured Information Standards (http://www.oasis-open.org/), IEC 61968: Common Information Model (CIM) / Distribution Management (http://www.iec.ch/smartgrid/standards/), and the NERC Critical Infrastructure Protection Program (http://www.nerc.com/page.php?cid=6|69).

[c] In other words, personnel with responsibilities for specific assets or classes of assets are involved in inventory, configuration management, and change management activities for those assets.

7. Personnel
    a. Responsibility and authority for the performance of ASSET activities is assigned to personnel [WORKFORCE]
    b. Personnel performing ASSET activities have the skills and knowledge needed to perform their assigned responsibilities [WORKFORCE]

MILX: Reserved for future use

Workforce Management (WORKFORCE)

Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of staff, commensurate with the risk to critical infrastructure and organizational objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Cybersecurity Responsibilities
    a. Cybersecurity responsibilities for the function are identified
2. Managing workforce lifecycle
    a. Personnel vetting (e.g., background checks, drug tests)is performed at hire for positions that have responsibilities for or access to the assets required for delivery of the function
3. Cybersecurity Knowledge, Skills, and Abilities
    a. Cybersecurity training is made available to personnel with cybersecurity responsibilities
4. Cybersecurity Awareness
    a. Cybersecurity awareness activities occur

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Cybersecurity Responsibilities
    a. Cybersecurity requirements for roles are established (e.g., separation of duties, least privilege)
    b. Cybersecurity responsibilities are assigned to specific roles, including external service providers
    c. Cybersecurity responsibilities are documented in position descriptions
2. Managing workforce lifecycle
    a. Personnel transfer and termination procedures are defined
    b. Personnel vetting is performed periodically for positions that have responsibilities for or access to the assets required for delivery of the function
3. Cybersecurity Knowledge, Skills, and Abilities
    a. Cybersecurity knowledge, skill, and ability gaps are identified
    b. Personnel with cybersecurity responsibilities complete continuing education and professional development
4. Cybersecurity Awareness
    a. Cybersecurity awareness activities occur in accordance with a defined awareness plan
    b. Cybersecurity awareness content is based on understanding of function-specific cybersecurity threats [THREAT][SITUATION]

5. Plan
    a. A documented plan is in place for WORKFORCE activities
    b. Standards and/or guidelines have been identified to inform WORKFORCE activities.
6. Stakeholders
    a. Stakeholders for WORKFORCE activities are identified and involved

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Cybersecurity Responsibilities
    a. Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate
    b. Cybersecurity responsibilities are included in job performance evaluation criteria
    c. Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage
2. Managing workforce lifecycle
    a. Risk designations are created based on risk analysis
    b. Risk designations are assigned to positions
    c. Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation
    d. Recruiting and retention are aligned to support cybersecurity workforce management objectives
    e. Succession planning is performed for personnel based on risk designation
    f. Security policy includes a formal disciplinary process and sanctions for employees who commit violations of security policy
3. Cybersecurity Knowledge, Skills, and Abilities
    a. Assessments of specific workforce skills are performed
    b. Assessments of the training program are performed
    c. Plan to address identified cybersecurity knowledge, skill, and ability gaps is maintained
    d. Personnel with cybersecurity responsibilities complete continuing education and professional development, consistent with job role and cybersecurity responsibilities
4. Cybersecurity Awareness
    a. Cybersecurity awareness content is based on an understanding of organization-specific (cross-function) cybersecurity threats [THREAT][SITUATION]
5. Policy
    a. WORKFORCE activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines
    c. WORKFORCE activities are periodically reviewed to ensure conformance with policy
6. Resources
    a. Adequate resources (people, funding, and tools) are provided to support WORKFORCE activities [CYBER]

7. Personnel
    a. Responsibility and authority for the performance of WORKFORCE activities is assigned to personnel
    b. Personnel performing WORKFORCE activities have the skills and knowledge needed to perform their assigned responsibilities

MILX: Reserved for future use

Identity and Access Management (ACCESS)

Identities are created and managed for entities that may be granted logical or physical access to the organization's assets. Access to the organization's assets is controlled, commensurate with the risk to critical infrastructure and organizational objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Identity Management
    a. Identities are provisioned for personnel and other entities who require access to assets (note that this does not preclude shared identities)
    b. Credentials are issued for personnel and devices that require access to assets (e.g., passwords, smart cards, certificates, keys)
    c. Identities are deprovisioned when no longer required
2. Access Management
    a. Access requirements, including those for remote access, are determined
    b. Access is granted to identities based on requirements (e.g.,)
    c. Access is revoked when no longer required

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Identity Management
    a. Standard procedures are implemented to provision and deprovision identities
    b. Identity repositories are periodically reviewed and updated to ensure validity (i.e. to ensure that the identities still need access)
    c. Credentials are periodically reviewed to ensure that they are associated with the correct entities
2. Access Management
    a. Access requests are reviewed and approved by the asset owner
    b. Standard procedures are implemented to grant and revoke access (e.g., Role-based access control)
    c. Access privileges are periodically reviewed and updated to ensure validity
    d. Least privilege and separation of duties principles are applied
3. Plan
    a. A documented plan is in place
    b. Standards and/or guidelines have been identified in the plan to inform ACCESS activities
4. Stakeholders
    a. Stakeholders for ACCESS activities are identified and involved

MIL3: Managed

1. Activities are guided by policies and governance
2. Activities are periodically reviewed to ensure they conform to policy
3. Adequate resources are provided to support the process (people, funding, and tools)
4. Responsibility and authority for performing the practice is clearly assigned to personnel
5. Personnel performing the practice have adequate skills and knowledge
6. Domain artifacts are controlled
7. Controls are periodically reviewed against identified standards

1. Identity Management
    a. Identity management is informed by risk analysis
    b. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access)
2. Access Management
    a. Access to assets is granted by the asset owner based on risk to the function
3. Cross-domain coordination
    a. Identity management is coordinated with WORKFORCE to ensure that personnel identities are valid
    b. Anomalous access attempts are monitored to inform situational awareness [SITUATION]
4. Policy
    a. ACCESS activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines
    c. ACCESS activities are periodically reviewed to ensure conformance with policy
5. Resources
    a. Adequate resources (people, funding, and tools) are provided to support ACCESS activities [CYBER]
6. Personnel
    a. Responsibility and authority for the performance of ACCESS activities is assigned to personnel [WORKFORCE]
    b. Personnel performing ACCESS activities have the skills and knowledge needed to perform their assigned responsibilities [WORKFORCE]

MILX: Reserved for future use

Risk Management (RISK)

Establish, operate, and maintain a cybersecurity risk management program to identify, analyze and mitigate cybersecurity risk to the organization and its related interconnected infrastructure and stakeholders.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Risk Strategy
    a. There is a notional risk management strategy
2. Sponsorship
    a. Management encourages personnel aware of cybersecurity risks to the function to communicate those risks
3. Risk Management Program
    a. Risk assessments and mitigation are performed

MIL2: Performed

1. Practices are performed according to a documented plan
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Risk Strategy
    a. There is a documented risk management strategy
    b. The strategy provides an approach for risk prioritization
2. Sponsorship
    a. A risk management program is established and endorsed by management
3. Risk Management Program
    a. Risk assessments and mitigation are performed in accordance with the risk management program
    b. Risks are identified, analyzed, disposed, and tracked to closure in accordance with the risk management program
    c. A network (IT and/or OT) architecture is used to support risk analysis
4. Plan
    a. A documented plan is in place for RISK activities [CYBER]
    b. Standards and/or guidelines have been identified to inform RISK activities
5. Stakeholders
    a. Stakeholders for RISK activities are identified and involved

MIL3: Managed

1. Activities are guided by policies and governance
2. Activities are periodically reviewed to ensure they conform to policy
3. Adequate resources are provided to support the process (people, funding, and tools)
4. Responsibility and authority for performing the practice is clearly assigned to personnel
5. Personnel performing the practice have adequate skills and knowledge
6. Domain artifacts are controlled
7. Controls are periodically reviewed against identified standards

1. Risk Strategy
    a. Organizational risk goals and objectives (tolerance for risk, risk avoidance approaches, risk parameter factors) are defined
    b. The risk management strategy is periodically updated to reflect the current threat environment [THREAT]
2. Sponsorship
    a. Risk governance is established
    b. Adequate resources (people, funding, and tools) are provided to support RISK activities [CYBER]
    c. The development and maintenance of RISK policies and guidelines is sponsored
3. Risk Management Program
    a. The risk management program defines and operates risk management policies and procedures that implement the Risk Strategy
    b. A current cybersecurity architecture is used to support risk analysis
    c. Risks are monitored and communicated to support situational awareness [SITUATION]
    d. Pre-defined states of operation are defined and invoked (manual or automated process) based on risk [SITUATION]
    e. An organization-specific risk taxonomy is documented and is used in RISK activities
4. Cross-domain coordination
    a. Risk assessment and disposition activities are integrated with threat and vulnerability identification and assessment (THREAT)
5. Policy
    a. RISK activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines
    c. RISK activities are periodically reviewed to ensure conformance with policy
6. Personnel
    a. Responsibility and authority for the performance of RISK activities is clearly assigned to personnel [WORKFORCE] [CYBER]
    b. Personnel performing RISK activities have adequate skills and knowledge [WORKFORCE]

MILX: Reserved for future use

Supply Chain and External Dependencies Management (DEPENDENCIES)

Establish and maintain controls to manage the cybersecurity risk associated with services and assets that are dependent on external entities, commensurate with the organization's business and security objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Dependency identification
    a. Important suppliers and other up-stream dependencies are identified (i.e. external parties on which the delivery of the function depend)
    b. Important down-stream dependencies are identified (i.e. external parties that are dependent on the delivery of the function)
2. Risk management
    a. Significant cybersecurity risks due to suppliers and other external dependencies are identified and addressed
3. Cybersecurity Requirements
    a. Cybersecurity requirements are considered when establishing relationships with external entities

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Dependency identification
    a. Important suppliers and up-stream dependencies are identified according to a defined practice
    b. Important down-stream dependencies are identified according to a defined practice
    c. Dependencies are prioritized based on established criteria
2. Risk management
    a. Cybersecurity risks due to suppliers and other external dependencies are identified according to a defined practice
    b. Identified external dependency cybersecurity risks are analyzed and disposed according to a defined practice
3. Cybersecurity Requirements
    a. Cybersecurity requirements are established for suppliers and up-stream dependencies according to a defined practice, including requirements for secure software development practices where appropriate
    b. Agreements with suppliers and other external entities include cybersecurity requirements
    c. Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements

d. Agreements with suppliers and other up-stream dependencies require notification of cybersecurity incidents related to the delivery of the product or service
e. Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements

4. Plan
   a. A documented plan is in place that addresses DEPENDENCY activities
   b. Standards and/or guidelines have been identified to inform DEPENDENCIES activities.
5. Stakeholders
   a. Stakeholders for DEPENDENCIES activities are identified and involved

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Dependency identification
   a. Bidirectional dependencies are identified
   b. Single-source dependencies are identified
2. Risk management
   a. Cybersecurity risks due to external dependencies are managed according to the organization's risk management criteria and process [RISK]
3. Cybersecurity Requirements
   a. Cybersecurity requirements are established for up-stream dependencies based on the organization's risk criteria
   b. Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended lifecycle of delivered products [THREAT]
   c. Acceptance testing of procured assets includes testing for cyber-security specifications (note this should be coordinated with change management activities in ASSET)
   d. Authoritative information sources are monitored to identify and avoid known sources of counterfeit parts and services
4. Cross-domain coordination
   a. Suppliers, vendors, and other up-stream dependencies are integrated into the information sharing process [SHARING]
5. Policy
   a. DEPENDENCIES activities are guided by documented policies in the organization
   b. Policies include compliance requirements for specified standards and/or guidelines
   c. DEPENDENCIES activities are periodically reviewed to ensure conformance with policy
6. Resources
   a. Adequate resources (people, funding, and tools) are provided to support DEPENDENCIES activities [CYBER]
7. Personnel
   a. Responsibility and authority for the performance of DEPENDENCIES activities is clearly assigned to personnel [WORKFORCE]

b. Personnel performing DEPENDENCIES activities have the skills and knowledge needed to perform their assigned responsibilities [WORKFORCE]

MILX: Reserved for future use

Threat and Vulnerability Management (THREAT)

Establish and maintain plans, procedures, and technologies to identify, analyze, and manage cybersecurity threats and vulnerabilities commensurate with the risk to critical infrastructure and organizational objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Threat management
    a. Cybersecurity threat information is gathered and interpreted for the function
    b. Threats that are considered important to the function are mitigated
2. Vulnerability management
    a. Cybersecurity vulnerability information is gathered and interpreted for the function
    b. Vulnerabilities that are considered important to the function are remediated
3. Cybersecurity patch management
    (Note this is a subset of vulnerability management and is treated separately here to reinforce that distinction)
    a. Patches that mitigate cybersecurity vulnerabilities are deployed [ASSET]

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Threat management
    a. Information sources to support threat management activities are identified and monitored (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors)
    b. Guidelines or criteria are established and used in the analysis and prioritization of identified threats
    c. Threats are addressed according to the prioritization criteria and mitigating actions are validated
2. Vulnerability management
    a. Information sources to support vulnerability management activities are identified and monitored
    b. Guidelines or criteria are established and used in the analysis and prioritization of identified vulnerabilities
    c. Vulnerabilities are addressed according to the prioritization criteria and remediation actions are validated
3. Cybersecurity patch management
    a. Information sources to support patch management activities are identified and monitored

b. Guidelines or criteria are established and used in the analysis and prioritization of cybersecurity patches (e.g., NIST Common Vulnerability Scoring System could be used for IT patches)
c. Patches are deployed according to the prioritization criteria (*Note prioritization criteria should include coverage of emergency patching*)

4. Plan
    a. A documented plan is in place for THREAT activities that addresses both information technology and operational technology for the function
    b. Standards and/or guidelines have been identified to inform THREAT activities
5. Stakeholders
    a. Stakeholders for THREAT activities are identified and involved

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Threat management
    a. Threat information is shared through participation in identified information sharing channels [SHARING]
    b. Analysis and prioritization of threats are informed by the function's risk criteria [RISK]
    c. Threat identification and analysis activities inform function's risk management activities [RISK]
2. Vulnerability management
    a. Vulnerability management activities are informed by the function's risk criteria [RISK]
    b. Vulnerability identification and analysis activities inform function's risk management activities [RISK]
    c. Vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)
3. Cybersecurity patch management
    a. Patch management activities are informed by the function's risk criteria [RISK]
4. Cross-domain coordination
    a. THREAT information is communicated within the function to support situational awareness [SITUATION]
5. Policy
    a. THREAT activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines.
    c. THREAT activities are periodically reviewed to ensure conformance with policy
6. Resources
    a. Adequate resources (people, funding, and tools) are provided to support THREAT activities [CYBER]

7. Personnel
    a. Responsibility and authority for the performance of THREAT activities is assigned to personnel [WORKFORCE] [CYBER]
    b. Personnel performing THREAT activities have adequate skills and knowledge [WORKFORCE]

MILX: Reserved for future use

Event and Incident Response, Continuity of Operations (RESPONSE)

Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and incidents, and to sustain critical functions throughout a cyber event or incident, commensurate with the risk to critical infrastructure and organizational objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Detect cybersecurity events
    a. Individuals who detect an anomalous event they believe may have cybersecurity implications, report the event to a clearly identified person or role in the function
2. Declare cybersecurity incidents
    a. Cybersecurity incident criteria are established based on the potential impact to the function
    b. Events are analyzed to identify and declare cybersecurity incidents
3. Respond to cybersecurity Incidents
    a. Actions are taken to respond to cybersecurity incidents to limit impact to the function and restore normal operations
    b. Incident response personnel are identified and roles are assigned
4. Continuity
    a. Assets that are important to the delivery of the function are identified (Note, this may be connected to or provided from ASSET]
    b. The activities necessary to sustain minimum operations of the function are identified
    c. The sequence of activities necessary to return the function to normal operation is identified

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Detect cybersecurity events
    a. Events are detected or reported according to a defined practice
    b. Events are logged and tracked according to a defined practice
2. Declare cybersecurity incidents
    a. Events are analyzed according to a defined practice
    b. Incidents are logged and tracked to closure according to a defined practice
    c. Cybersecurity incident declaration criteria are periodically updated according to a defined practice
    d. Events are analyzed to identify and declare cybersecurity incidents according to a defined practice

3. Respond to cybersecurity incidents
    a. Incident response is performed according defined procedures that address all phases of the incident lifecycle (e.g., triage, handling, communication, coordination, and closure)
    b. Incident response procedures are exercised
    c. Training is conducted for incident response teams
4. Continuity
    a. Business impact analyses are conducted according to defined practices to inform the development of continuity plans
    b. Recovery time objectives are established for the function
    c. Continuity plans are developed to sustain and restore operation of the function according to a defined practice
    d. Continuity plans are evaluated and exercised
5. Plan
    a. A documented plan is in place that addresses RESPONSE activities
    b. Standards and/or guidelines have been identified to inform RESPONSE activities.
6. Stakeholders
    a. Stakeholders for RESPONSE activities are identified and involved

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Detect cybersecurity events
    a. Event information is correlated to support incident analysis by identifying patterns, trends, and other common features
    b. Cybersecurity event detection is informed by THREAT and RISK information (e.g., event detection is tuned to help detect known threats and monitor for identified risks)
    c. Cybersecurity event detection is enabled by SITUATION activities
2. Declare cybersecurity incidents
    a. Declared incidents are correlated to support the discovery of patterns, trends, and other common features
    b. Incident declaration criteria are periodically updated based on THREAT, SITUATION, and RISK information
3. Respond to cybersecurity incidents
    a. Cybersecurity incident root-cause analysis and lessons-learned activities are performed as part of the defined process
    b. Procedures are followed to coordinate and collaborate with law enforcement when appropriate, including support for evidence collection and preservation
    c. Incident response personnel participate in community cybersecurity exercises (e.g., table top, simulated incidents)
    d. The incident response process is periodically reviewed and updated
    e. Incident response activities are coordinated with relevant external entities [SHARING, DEPENDENCIES]

f.

4. Continuity
    a. Business impact analyses are periodically reviewed and updated
    b. The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly
    c. Continuity plans are periodically reviewed and updated
5. Cross-domain
    a. RESPONSE information is shared with relevant external entities (e.g., ES-ISAC, trade associations, vendors) [SHARING] [DEPENDENCIES]
    b. RESPONSE activities are coordinated with ASSET activities to ensure that restored assets are configured appropriately and inventory information is updated
6. Policy
    a. RESPONSE activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines.
    c. RESPONSE activities are periodically reviewed to ensure conformance with policy
    d. Policy and procedures for reporting incident information to designated authorities conform with applicable laws, regulations, and contractual agreements [CYBER]
7. Resources
    a. Adequate resources (people, funding, and tools) are provided to support RESPONSE activities [CYBER]
8. Personnel
    a. Responsibility and authority for the performance of RESPONSE activities is assigned to personnel [WORKFORCE]
    b. Personnel performing RESPONSE activities have the skills and knowledge needed to perform their assigned responsibilities [WORKFORCE]

MILX: Reserved for future use

Situational Awareness (SITUATION)

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use power system and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture, commensurate with the risk to critical infrastructure and organizational objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Logging
    a. Logging capabilities are identified and selected capabilities are activated
    b. A consistent level of logging is occurring for assets important to the function [ASSET]
2. Monitoring
    a. Cybersecurity monitoring activities are performed (e.g. periodic reviews of log data)
    b. Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event
3. Awareness
    a. A local operating picture exists for the function

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Logging
    a. Logging requirements have been defined and documented for all assets of selected classes and/or priority [ASSET]
    b. Logging is performed in compliance with the documented requirements
    c. Logs are managed with consistency within the function
    d. Log data are being aggregated within the function
2. Monitoring
    a. Monitoring and analysis requirements have been defined and documented
    b. Monitoring and analysis is performed in compliance with the documented requirements
    c. Alarms and alerts are implemented
3. Awareness
    a. A common operating picture exists across functions
    b. The cybersecurity operations of the function are informed based on the common operating picture
4. Plan
    a. A documented plan is in place for SITUATION activities
    b. Standards and/or guidelines have been identified to inform SITUATION activities

5. Stakeholders
    a. Stakeholders for SITUATION activities are identified and involved

MIL3: Managed

1. Activities are guided by policies and governance
2. Activities are periodically reviewed to ensure they conform to policy
3. Adequate resources are provided to support the process (people, funding, and tools)
4. Responsibility and authority for performing the practice is clearly assigned to personnel
5. Personnel performing the practice have adequate skills and knowledge
6. Domain artifacts are controlled
7. Controls are periodically reviewed against identified standards

1. Logging
    a. Logging requirements are based on the risk to the function [RISK]
    b. Logging is integrated with other business and security processes
2. Monitoring
    a. Monitoring requirements are based on the risk to the function [RISK]
    b. Monitoring is integrated with other business and security processes [RESPONSE][ACCESS][ASSET]
    c. Alarms and alerts are defined by severity level for both power system and cybersecurity information
3. Awareness
    a. Common operating picture incorporates information from external sources (including external entities on which the function depends) [DEPENDENCIES]
    b. Pre-defined states of operation are defined and invoked (manual or automated process) based on the common operating picture
4. Cross-domain coordination
    a. Common operating picture is shared with stakeholders external to the function [SHARING][DEPENDENCIES]
5. Policy
    a. SITUATION activities are guided by documented policies in the organization
    b. Policies include compliance requirements for specified standards and/or guidelines
    c. SITUATION activities are periodically reviewed to ensure conformance with policy
6. Resources
    a. Adequate resources (people, funding, and tools) are provided to support SITUATION activities [CYBER]
7. Personnel
    a. Responsibility and authority for the performance of SITUATION activities is assigned to personnel [WORKFORCE] [CYBER]
    b. Personnel performing SITUATION activities have the skills and knowledge needed to perform their assigned responsibilities [WORKFORCE]

MILX: Reserved for future use

Information Sharing and Communications (SHARING)

Establish and maintain relationships with internal and external entities to share information, including threats and vulnerabilities, to reduce risk and increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Communication
    a. The key stakeholders (including connected utilities) with which information needs to be shared have been identified
    b. Communication with key stakeholders is performed
2. Analysis
    a. Analysis of shared information is performed
3. Coordination
    a. Responsibility for the collection of shared cybersecurity information is assigned

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Communication
    a. Communication with key stakeholders is based on documented communication strategies within functional areas
    b. Contracts and agreements with third parties incorporate sharing of cybersecurity threat information
    c. Information reporting requirements are identified
2. Analysis
    a. Analysis of shared information occurs based on defined procedures
    b. Procedures are in place to create action plans in response to information received [THREAT] [RESPONSE]
3. Coordination
    a. Cybersecurity information is shared across functional areas
    b. Trusted information sharing partners are identified
    c. The function participates with information sharing and analysis centers [THREAT] [RESPONSE]
4. Plan
    a. A documented plan is in place for SHARING activities [RESPONSE]
    b. The plan addresses standard operations and emergency operations
    c. Standards and/or guidelines have been identified to inform SHARING activities.

5. Stakeholders
    a. Stakeholders for SHARING activities are identified and involved

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Communication
    a. Information shared supports situational awareness at organization, regional, and national levels [SITUATION]
2. Analysis
    a. Technical sources are identified that can be accessed to gain expert insights
    b. Procedures are in place to analyze and de-conflict received information
3. Coordination
    a. A robust network of internal and external trust relationships (both formal and informal) has been established to vet and validate information about cyber events
    b. There is a strategy or policy and procedure for incident coordination with external partners & stakeholders [RESPONSE]
    c. Provisions are established and maintained to enable secure sharing of sensitive or classified information
4. Policy
    a. SHARING activities are guided by documented policies in the organization
    b. Policies for information sharing address protected information, ethical use and sharing of information, including as appropriate sensitive and classified information
    c. Policies include compliance requirements for specified standards and/or guidelines
    d. SHARING activities are periodically reviewed to ensure conformance with policy
5. Resources
    a. Adequate resources (people, funding, and tools) are provided to support SHARING activities [CYBER]
6. Personnel
    a. Responsibility and authority for the performance of SHARING activities is assigned to personnel [WORKFORCE] [RESPONSE] [CYBER]
    b. Personnel performing SHARING activities have the skills and knowledge needed to perform their assigned responsibilities[WORKFORCE]

MILX: Reserved for future use

Cybersecurity Program Management (CYBER)

Establish and maintain a cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

MIL0: Incomplete

—

MIL1: Initiated *1. Initial practices are performed but may be ad hoc*

1. Strategy
    a. The organization's strategic objectives are generally understood among senior management
    b. The organization's cybersecurity objectives are generally understood among the personnel performing cybersecurity activities, but may not be connected to the organization's strategic objectives
2. Sponsorship
    a. Some resources (people, tools, and funding) are provided to support cybersecurity activities, but may be compartmentalized (or siloed)
    b. Senior management is aware of cybersecurity concerns and provides at least vocal sponsorship for cybersecurity activities
3. Cybersecurity Program
    a. Cybersecurity activities are performed by individuals in the organization and may be compartmentalized
4. Cybersecurity Architecture
    a. A strategy to architecturally isolate the organization's IT systems from OT systems is implemented

MIL2: Performed *1. Practices are performed according to a documented plan*
2. Stakeholders of the practice are identified and involved
3. Standards and/or guidelines have been identified to guide the implementation of the practices

1. Strategy
    a. The organization's strategic objectives are documented and well-understood throughout the organization
    b. The organization's cybersecurity strategy and priorities are documented and aligned with the organization's strategic objectives
2. Sponsorship
    a. The importance and value of cybersecurity activities is regularly communicated by senior management
    b. Activities to support and develop a culture of cybersecurity in the organization are sponsored [WORKFORCE]
    c. The creation and maintenance of a cybersecurity program plan is sponsored by the organization

   d. If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program

3. Cybersecurity program
   a. Cybersecurity requirements are developed for key operational systems and assets
   b. A cybersecurity program is established and maintained to provide security for IT and OT systems, networks, and data, consistent with the cybersecurity strategy and requirements
   c. Industry activities are monitored to identify emerging cybersecurity trends, issues, standards, and initiatives [SHARING]

4. Cybersecurity architecture
   a. A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy and priorities
   b. Architectural segmentation and isolation is maintained according to a documented plan

5. Plan
   a. Documented plans are in place that guide the implementation and performance of cybersecurity activities across the organization, including communication and reporting plans
   b. Standards and/or guidelines have been identified to inform CYBER activities

6. Secure Software Development
   a. Software to be deployed on assets of selected classes and/or priority is developed using secure software development practices [ASSET]

7. Stakeholders
   a. Stakeholders for CYBER activities are identified and involved

MIL3: Managed	*1. Activities are guided by policies and governance* *2. Activities are periodically reviewed to ensure they conform to policy* *3. Adequate resources are provided to support the process (people, funding, and tools)* *4. Responsibility and authority for performing the practice is clearly assigned to personnel* *5. Personnel performing the practice have adequate skills and knowledge* *6. Domain artifacts are controlled* *7. Controls are periodically reviewed against identified standards*

1. Strategy
   a. The development and implementation of a cybersecurity strategy and its integration with organizational objectives is required by policy
   b. Cybersecurity strategy and objectives address the organization's role in critical infrastructure

2. Sponsorship
   a. Adequate funding and other resources (i.e. people and tools) are provided to establish and operate a cybersecurity program
   b. The development and maintenance of cybersecurity policies and guidelines is sponsored

3. Cybersecurity program
   a. DOMAINS activities are integrated, coordinated, and aligned into a systematic policy and procedure to ensure that the organization's cybersecurity objectives and strategy are addressed
   b. Organization monitors and participates in selected emerging cybersecurity standards or initiatives to support cybersecurity strategies and objectives

   c. Coordination occurs with organization's compliance efforts to support ongoing achievement of any cybersecurity compliance requirements

4. Cybersecurity architecture
   a. Architectural segmentation and isolation strategies are informed by the organization's risk tolerance
   b. Cybersecurity architecture is routinely updated as may be required to keep it current and to address new requirements

5. Secure Software Development
   a. Policies require that software to be deployed on assets above a priority threshold be developed using secure software development practices [ASSET]

6. Policy
   a. CYBER activities are guided by documented policies in the organization
   b. Policies include compliance requirements for specified standards and/or guidelines
   c. Policies include compliance requirements for any applicable regulations
   d. CYBER activities are periodically reviewed to ensure conformance with policy

7. Personnel
   a. Responsibility and authority for the performance of CYBER activities is clearly assigned to personnel [WORKFORCE]
   b. Personnel performing CYBER activities have adequate skills and knowledge [WORKFORCE]

MILX: Reserved for future use

5 Glossary

5.1 Referenced Sources of Definitions

The following documents have been referenced for terms defined in this glossary.

[CNSSI 4009] Committee on National Security Systems, National Information Assurance (IA) Glossary, CNSSI 4009 Instructions no. 4009, April 26, 2010.

[FIPS 200] FIPS-200: Minimum Security Requirements for Federal Information and Information Systems, National Institute of Standards and Technology, 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[NDIA ESA] National Defense Industrial Association System Assurance Committee, Engineering for System Assurance, National Defense Industry Association (NDIA), September 2008.

[NIST 800-53] Security and Privacy Controls for Federal Information Systems and Organization, NIST Special Publication 800-53, Revision 4, Initial Public Draft, February 2012. http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-Rev.%204

[NIST 800-61] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-61, Revision 2 (Draft), January 2012. http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf

[NISTIR 7622] Marianne Swanson, Nadya Bartol, and Rama Moorthy, Piloting Supply Chain Risk Management for Federal Information Systems, Draft NISTIR 7622, June 2010. http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf.

[NISTIR 7628] Interagency Report 7628: Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology, Volumes 1-3, 2010, http://csrc.nist.gov/publications/PubsNISTIRs.html

5.2 Notes Regarding Glossary Development

1. Some of the definitions sourced from the named references needed to be generalized somewhat to make them applicable beyond an information systems perspective, to include concepts applicable to Electricity Subsector operational technology (OT), or to particularize examples to the electricity sector. For example: (The second definition for "Access Control" is an adaptation by the model team for use here).

Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).	CNSSI 4009
Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services, and for gaining operational control; and 2) to enter specific physical facilities (e.g., a substation, control center, or a locked equipment cabinet).	Adapted from CNSSI 4009

2. The model team will continue to search [NISTIR 7628] for additional electric-sector specific definitions to include here. Many definitions in [NISTIR 7628] are distributed throughout volume 1, which makes finding them labor intensive

3. ***Reviewers of this draft are encouraged to offer additional sources and specific definitions (including source) in their comments.***

5.3 Glossary Terms

Term	Definition	Source
Access	Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.	CNSSI 4009
Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities ...	CNSSI 4009

Access Control Mechanism	Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.	
Accountability	Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.	CNSSI 4009
Authentication	The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. NIST SP 800-53: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS 200]	CNSSI 4009
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).	NIST 800-53
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.	CNSSI 4009
Access Control Enforcement	Data integrity and confidentiality are enforced by access controls. When the subject requesting access has been authorized to access particular processes, it is necessary to enforce the defined security policy (e.g., MAC or DAC). These policy-based controls are enforced via access control mechanisms distributed throughout the system (e.g., MAC sensitivity labels; DAC file permission sets, access control lists, roles, user profiles). The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security)	
Certification	Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. See security control assessment.	CNSSI 4009
Change Management and Configuration Management	Configuration management means that assets are managed to a configuration baseline to ensure that similar assets remain in a common configuration. Change management applies to both changes to specific configurations and also more broadly to changes in the asset landscape (deploying a new class of assets, or changing out a major asset). In the context of software development, the configuration of the source code base should be managed to ensure that stable and consistent configurations are released. Changes to the source code should be subject to change control procedures, reviews, and tests prior to committing those changes to a new software configuration (which may also be called a release or a version).	

Contingency Plan	Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or Disaster Recovery Plan for major disruptions.	CNSSI 4009
Continuity of Operations Plan (COOP)	Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan.	CNSSI 4009
Critical Energy Infrastructure Information (CEII)	Critical Energy Infrastructure Information is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: relates details about the production, generation, transmission, or distribution of energy; could be useful to a person planning an attack on critical infrastructure; is exempt from mandatory disclosure under the Freedom of Information Act; and gives strategic information beyond the location of the critical infrastructure.	
Cybersecurity risk	TBD	
Disaster Recovery Plan (DRP)	Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan.	CNSSI 4009
Event	An *event* is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. *Adverse events* are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. *TBD – Need to generalize for OT.*	NIST 800-61
Federated Identity Management	Managing identities and access across organizational boundaries in a standardized manner (including standardized policies, procedures, and technologies). *TBD – need authoritative source for definition.*	

Generally Accepted Privacy Principles (GAPP)	Generally Accepted Privacy Principles. Privacy principles and criteria developed and updated by the AICPA and Canadian Institute of Chartered Accountants to assist organizations in the design and implementation of sound privacy practices and policies.	NISTIR 7628 Vol. 3, Glossary
Hacker	In common usage, a hacker is a person who breaks into computers and/or computer networks, usually by gaining access to administrative controls. Proponents may be motivated by diverse objectives from the shear entertainment value they find in the challenge of circumventing computer/network security to political or other ends. Hackers are often unconcerned about the use of illegal means to achieve their ends. Out-and-out cyber-criminal hackers are often referred to as "crackers."	NISTIR 7628 Vol. 3, Glossary
Identity	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	CNSSI 4009
Identity-Based Access Control	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.	CNSSI 4009
Incident	A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An "imminent threat of violation" refers to a situation in which the organization has a factual basis for believing that a specific incident is about to occur. For example, the antivirus software maintainers may receive a bulletin from the software vendor, warning them of new malware that is rapidly spreading across the Internet. *TBD –Need to generalize for OT.*	NIST 800-61 (computer security incident)
Inside(r) Threat	An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.	CNSSI 4009
Integrator	A person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems function together, a practice known as System Integration. Systems integrators may work in many fields but the term is widely used in the information technology (IT) field.	
Intrusion	Unauthorized act of bypassing the security mechanisms of a system.	CNSSI 4009
Intrusion Detection Systems (IDS)	Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations).	CNSSI 4009

Intrusion Detection Systems (IDS), (host-based)	IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.	CNSSI 4009
Intrusion Detection Systems (IDS), (network-based)	IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.	CNSSI 4009
Intrusion Prevention System (IPS)	System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.	CNSSI 4009
ISO/IEC27001	International Organization for Standardization/International Electrotechnical Commission Standard 27001. A auditable international standard that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It uses a process approach for protection of critical information.	NISTIR 7628 Vol. 3, Glossary
Multi-Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See *Authenticator*.	NIST 800-53
Personal Information	Information that reveals details, either explicitly or implicitly, about a specific individual’s household dwelling or other type of premises. This is expanded beyond the normal "individual" component because there are serious privacy impacts for all individuals living in one dwelling or premise. This can include items such as energy use patterns or other types of activities. The pattern can become unique to a household or premises just as a fingerprint or DNA is unique to an individual.	NISTIR 7628 Vol. 3, Glossary
Personally Identifiable Information (PII)	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.	CNSSI 4009
Privacy Impact Assessment (PIA)	A process used to evaluate the possible privacy risks to personal information, in all forms, collected, transmitted, shared, stored, disposed of, and accessed in any other way, along with the mitigation of those risks at the beginning of and throughout the life cycle of the associated process, program or system.	

Protected Critical Infrastructure Information (PCII)	The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security and other federal, state and local analysts use PCII to, 1) analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures.	
Provisioning / Deprovisioning	Granting (provisioning) and removing or revoking (deprovisioning) access based on identities and roles. *TBD - Need authoritative source for definition.*	
Public-key cryptography	A cryptographic approach that involves the use of asymmetric key algorithms instead of or in addition to symmetric key algorithms. Unlike symmetric key algorithms, it does not require a secure initial exchange of one or more secret keys to both sender and receiver.	NISTIR 7628 Vol. 3, Glossary
Remote Access	Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). NIST 800-53: Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).	CNSSI 4009
Resilience/Robustness	The ability of an Information Assurance entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.	CNSSI 4009 (robustness)
Risk Assessment	The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). NIST SP 800-53: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.	CNSSI 4009

Risk Management	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall risk management program. NIST SP 800-53: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system, and includes: 1. the conduct of a risk assessment; 2. the implementation of a risk mitigation strategy; and 3. employment of techniques and procedures for the continuous monitoring of the security state of the information system.	CNSSI 4009
Role	A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.	CNSSI 4009
Role-Based Access Control (RBAC)	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.	CNSSI 4009
Service Level Agreement (SLA)	Defines the specific responsibilities of the service provider and sets the customer expectations.	CNSSI 4009
Single Sign-on	A property of access control of multiple, related, but independent software systems. With this property a user/device logs in once and gains access to all related systems without being prompted to log in again at each of them.	NISTIR 7628 Vol. 3, Glossary
Situational Awareness	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.	CNSSI 4009
Social Engineering	The act of manipulating people into performing actions or divulging confidential information. The term typically applies to trickery or deception being used for purposes of information gathering, fraud, or computer system access.	NISTIR 7628 Vol. 3, Glossary

Supply Chain	The set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers. [Engineering for System Assurance, National Defense Industry Association (NDIA), Sep 2008.] The supply chain encompasses the full product life cycle and includes design, development, and acquisition of custom or commercial off-the-shelf (COTS) products, system integration, system operation (in its environment), and disposal. People, processes, services, products, and the elements that make up the products wholly impact the supply chain.	NISTIR 7622
Symmetric cipher	Cryptography solution in which both parties use the same key for encryption and decryption, hence the encryption key must be shared between the two parties before any messages can be decrypted.	NISTIR 7628 Vol. 3, Glossary
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.	CNSSI 4009
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	CNSSI 4009
Threat Assessment	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	CNSSI 4009
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.	CNSSI 4009
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.	CNSSI 4009

References

Source	ASSET	WORKFORCE	ACCESS	RISK	DEPENDENCIES	THREAT	RESPONSE	SITUATION	SHARING	CYBER
Accenture 2011 Global Risk Management Study: Utilities Industry Report				●						
Article "Improving Security for SCADA Systems" – Hentea 2008				●						
AS/NZS 4360:2004 "Risk Management, Standard" http://www.ucop.edu/riskmgt/erm/documents/as_stdrds4360_2004.pdf				●						
BSIMM						●				
Building A Cyber Supply Chain Assurance Reference Model http://www.saic.com/news/resources.asp?rk=1					●					
CERT-RMM, Asset Definition and Management (ADM) and Technology Management (TM) process areas	●									
CERT-RMM, External Dependencies Management process area					●					
CERT-RMM, Incident Management and Control (IMC) process area							●			
CERT-RMM, People Management (PM), Human Resource Management (HRM), and Organizational Training and Awareness (OTA) process areas		●								
CERT-RMM, Vulnerability Analysis and Resolution process area						●				
CFATS - RBPS 8	●						●			
Critical Energy Infrastructure Information (CEII) http://www.ferc.gov/legal/ceii-foia/ceii.asp									●	
Cross-Sector Roadmap for Cybersecurity of Control Systems						●				
DHS Cybersecurity Procurement Language for Control Systems					●					

Source	ASSET	WORKFORCE	ACCESS	RISK	DEPENDENCIES	THREAT	RESPONSE	SITUATION	SHARING	CYBER
http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf										
DHS ICS-CERT							●			
DHS ICSJWG									●	
Engineering for System Assurance, National Defense Industry Association (NDIA), Sep 2008					●					
ENISA Users guide		●								
ES-ISAC							●		●	
FIPS 199	●									
Handbook for Computer Security Incident Response Teams (CSIRTs) - Carnegie Mellon							●			
http://www.cert.org/csirts/csirt_faq.html	●						●			
http://www.shrm.org		●								
http://www.us-cert.gov/	●						●			
http://www.us-cert.gov/control_systems/ics-cert/	●						●			
https://dspace.lib.cranfield.ac.uk/bitstream/1826/2797/1/MacGillivray_Thesis.pdf				●						
IACMM – Process Area 4 and 5						●				
ICS-CERT Fly away team checklists and agreement	●									
IEEE 13335-1996 "Network Risk Calculation" original source document not freely available http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5348500				●						

Source	ASSET	WORKFORCE	ACCESS	RISK	DEPENDENCIES	THREAT	RESPONSE	SITUATION	SHARING	CYBER
Incident Response Plan - Template for Breach of Personal Information - AICPA							●			
ISO 27005:2008 "A Standard-Based Approach to IT Risk Management" http://www.jbwgroup.com/documents/ISO27005forSecure360updatedon10-22-08.pdf - link to a presentation of content - original source document not freely available.				●						
ISO/IEC 21827			●			●				
ISO/IEC 27001			●							
ISO/IEC 27002	●		●			●				
Marianne Swanson, Nadya Bartol, and Rama Moorthy, Piloting Supply Chain Risk Management for Federal Information Systems, Draft NISTIR 7622, June 2010. http://csrc.nist.gov/publications/drafts/nistir-7622/draft-nistir-7622.pdf					●					
NASA Risk Management Maturity Model				●						
NERC CIP-001									●	
NERC CIP-004		●							●	
NERC CIP-008							●		●	
NERC CIP-009							●			
NERC Security Guideline for Protecting Sensitive Information http://www.nerc.com/docs/cip/sgwg/Protecting%20Sensitive%20Information%20Guideline%20Draft%20Revision%208-30-11%20v04.pdf (v4 has not yet been approved by FERC)									●	
NERC Threat and Incident Reporting Security Guideline http://www.nerc.com/files/Incident-Reporting.pdf									●	

Source	ASSET	WORKFORCE	ACCESS	RISK	DEPENDENCIES	THREAT	RESPONSE	SITUATION	SHARING	CYBER
NERC-CIP 002	●		●			●				
NESCO						●	●	●	●	
NISITIR 7628 Volume III						●				
NIST 800-16		●								
NIST 800-30 "Risk Management Guide for Information Systems" http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf				●						
NIST SP800-137								●		
NIST SP800-37								●		
NIST SP800-50		●								
NIST SP800-53	●	●	●			●	●			
NIST SP800-61 Computer Security Incident Handling Guide - NIST							●			
NIST SP800-82 Guide to Industrial Control Systems (ICS) Security – NIST							●			
NIST SP800-83 Guide to Malware Incident Prevention and Handling – NIST							●			
NIST SP800-86 Guide to Integrating Forensic Techniques into Incident Response - NIST							●			
NISTIR 7628							●			
NISTIR 7628 Volume I	●		●							
NRECA InteroperabilityandCyberSecurityPlan[1].pdf								●		
Protected Critical Infrastructure Information (PCII)									●	

Source	ASSET	WORKFORCE	ACCESS	RISK	DEPENDENCIES	THREAT	RESPONSE	SITUATION	SHARING	CYBER
http://www.dhs.gov/files/programs/gc_1193089801658.shtm										
State of the Practice of Computer Security Incident Response Teams (CSIRTs) - Carnegie Mellon							●			
The DOE Electricity Sector Cybersecurity Risk Management Process (RMP)				●						
The IACCM Business Risk Management Maturity Model (BRM3)				●						
The OECD paper "Reducing Systemic Cybersecurity Risk" addresses monitoring as a core component of security strategy.								●		
The Open Group Open Information Security Management Maturity Model (O-ISM3)				●						
The RIMS Risk Maturity Model (RMM) for Enterprise Risk Management				●						
The Systems Security Engineering Capability Maturity Model 3.0 - addresses monitoring as a core component of security engineering.								●		
U.S. Department of Energy, Office of Energy Assurance, OE-417 http://www.oe.netl.doe.gov/oe417.aspx									●	
White paper by SANS on "Securing Modern Grid" series				●						

Notices

This material is based upon work funded and supported by the Department of Energy and the Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.