OMB Control Number : xxxx-xxxx

Electricity Subsector Cybersecurity Risk Management Maturity Initiative

FINAL
PILOT EVALUATION QUESTIONNAIRE

Disclaimer:
Completed form should be considered sensitive and protected accordingly.

Fillable PDF Form - version 2012-05-10

Contents

Expiration Date: DD-MM-YYYY

Part A: Information about the Organization

NOTE: Questions 1 and 2 are part of the Draft Pilot Evaluation Question Set but do not have input fields as this data will not be collected during pilot evaluations.

1. Organization completing this questionnaire (include division if applicable)
   a. Name
   b. Address
   c. Is the organization being assessed a subset of the overall organization?
   d. If yes, please include the name of the overall organization

2. Contact information for the person responsible for completing this questionnaire
   a. Name
   b. Email address
   c. Phone

3. Which of the following best characterizes your organization's ownership structure?
   ○ a. Investor-owned
   ○ b. Cooperative
   c. Government-owned by
      ○ i. Municipality/City
      ○ ii. State
      ○ iii. Federal government

4. Which electricity functions are performed by your organization (select all that apply):
   ☐ a. Generation
   ☐ b. Transmission
   ☐ c. Distribution
   ☐ d. Markets
   ☐ e. Other: _____

5. For which function is this questionnaire being completed (select one)?
   a. Generation
      If Generation is selected, please provide your non-nuclear generation capacity in megawatts: _____
   b. Transmission
      If Transmission is selected, please provide the total generation capacity connected to your transmission system in megawatts: _____
   c. Distribution
      If Distribution is selected, please provide your customer meter count: _____

Part B: Questions by Domain

Answer Scale

To complete each question, select a response from the following scale that best describes the extent to which the practice is implemented for the function selected (generation, transmission, distribution, or markets).

4-point answer scale	The organization's performance of the practice described in the model is …
Fully implemented	Complete
Largely implemented	Complete, but with a recognized opportunity for improvement
Partially implemented	Incomplete; there are multiple opportunities for improvement
Not implemented	Absent; the practice is not performed in the organization

Scoring Process

The model 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." The Maturity Indicator Levels are:

MIL0: Incomplete
MIL1: Initiated
MIL2: Performed
MIL3: Managed
MILX: Reserved for future use

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. 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 MIL levels are cumulative within each domain; 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.

Completion of a MIL is computed from answer input provided for the questions presented in the ten domains in Part B of this document. Each question describes a characteristic that can be answered with the four point answer scale. The characteristics are assigned scores based on the answer selected. The scores are assigned as follows:

'Fully Implemented' characteristic = Complete
'Largely Implemented' characteristic = Complete
'Partially Implemented' characteristic = Incomplete
'Not Implemented' characteristic = Incomplete

ASSET Domain

Asset, Change, and Configuration Management

Manage the organization's operational technology (OT) assets, information technology (IT) assets, and communications 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, and
- Manage changes to assets and to the asset inventory.

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **asset inventory**.
   a. There is an inventory of assets that are important to the delivery of the function — TBD
   b. 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) — TBD
   c. Inventoried assets are prioritized (e.g., critical versus noncritical or a more complex range) based on their role — TBD
   d. The asset inventory is current and complete for assets of defined categories that are selected based on risk analysis — TBD
   e. Asset prioritization is informed by risk analysis (i.e., a formal or structured risk analysis is used as the basis of prioritization) — TBD

2. Please rate your implementation of the following activities associated with **asset 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) — TBD
   b. Configuration baselines are established and kept current for high priority assets — TBD
   c. Configuration of assets are monitored for consistency with baselines — TBD
   d. Configuration baselines are designed to satisfy cybersecurity objectives — TBD
   e. Modifications to configuration baselines are subject to defined change management policies — TBD

ASSET

3. Please rate your implementation of the following activities associated with **asset change management**.

a. Changes to inventoried assets are evaluated before being implemented	TBD
b. Changes to inventoried assets are logged	TBD
c. Change management practices address the full lifecycle of assets (i.e., acquisition, deployment, operation, retirement)	TBD
d. Changes to assets are tested prior to being deployed	TBD
e. Changes to assets are tested for cybersecurity impact prior to being deployed	TBD
f. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)	TBD

4. Please rate your implementation of the following activities associated with planning and managing ***Asset, Change, and Configuration Management*** activities.

a. One or more plans or procedures are in place that guide the activities	TBD
b. One or more standards and/or guidelines have been identified to inform the activities	TBD
c. One or more policies are in place that guide the activities	TBD
d. The policies include compliance requirements for specified standards and/or guidelines	TBD
e. The activities are periodically reviewed to ensure conformance with the policy	TBD
f. Stakeholders are identified and involved in the activities	TBD
g. Resources (people, funding, and tools) are provided to support the activities	TBD
h. Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i. Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

RISK Domain

Risk Management

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.

- Strategy
- Sponsorship
- Program

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **risk management strategy**.
   a. There is a notional risk management strategy TBD
   b. There is a documented risk management strategy TBD
   c. The strategy provides an approach for risk prioritization TBD
   d. Organizational risk goals and objectives (e.g., tolerance for risk, risk avoidance approaches, risk parameter factors) are defined TBD
   e. The risk management strategy is periodically updated to reflect the current threat environment TBD

2. Please rate your implementation of the following activities associated with **risk sponsorship**.
   a. Management encourages personnel who discover or become aware of cybersecurity risks to the function to communicate those risks TBD
   b. A risk management program has been established and endorsed by management TBD
   c. Risk governance has been established (i.e., senior management has established goals, sponsorship, and accountability for the function's Risk Management activities, and periodically reviews performance to ensure that strategic goals are being achieved). TBD
   d. The development and maintenance of Risk Management policies and guidelines are sponsored TBD

RISK

3. Please rate your implementation of the following activities associated with **the risk management program**.

a.	Risk assessments and mitigation are performed	TBD
b.	Risk assessments and mitigation are performed in accordance with the risk management program's documented plan	TBD
c.	Risks are identified, analyzed, disposed, and tracked to closure in accordance with the risk management program	TBD
d.	A network (IT and/or OT) architecture is used to support risk analysis	TBD
e.	The risk management program defines and operates risk management policies and procedures that implement the Risk Strategy	TBD
f.	A current cybersecurity architecture is used to support risk analysis	TBD
g.	Risks are monitored and communicated to support situational awareness	TBD
h.	Pre-defined states of operation are defined and invoked (manual or automated process) based on risk	TBD
i.	An organization-specific risk taxonomy is documented and is used in Risk Management activities	TBD

4. Please rate your implementation of the following activities associated with planning and managing **Risk Management activities**.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	One or more standards and/or guidelines have been identified to inform the activities	TBD
c.	One or more policies are in place that guide the activities	TBD
d.	The policies include compliance requirements for specified standards and/or guidelines	TBD
e.	The activities are periodically reviewed to ensure conformance with the policy	TBD
f.	Stakeholders are identified and involved in the activities	TBD
g.	Resources (people, funding, and tools) are provided to support the activities	TBD
h.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

ACCESS Domain

Identity and Access Management

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.

- Identity management
- Access management

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **identity management activities**.
   a. Identities are provisioned for personnel and other entities who require access to assets (note that this does not preclude shared identities) TBD
   b. Credentials are issued for personnel and devices that require access to assets (e.g., passwords, smart cards, certificates, keys) TBD
   c. Identity repositories are periodically reviewed and updated to ensure validity (i.e. to ensure that the identities still need access) TBD
   d. Identities are deprovisioned when no longer required TBD
   e. Standard procedures are implemented to provision and deprovision identities TBD
   f. Credentials are periodically reviewed to ensure that they are associated with the correct entities TBD
   g. Identity management is informed by risk analysis TBD
   h. Requirements for credentials are informed by the function's risk criteria (e.g., multifactor credentials for higher risk access) TBD
   i. Identity management activities are coordinated with Workforce Management activities to ensure that personnel identities are valid TBD

ACCESS

2. Please rate your implementation of the following activities associated with **access management activities.**

a.	Access requirements, including those for remote access, are determined	TBD
b.	Access is granted to identities based on requirements	TBD
c.	Access is revoked when no longer required	TBD
d.	Access requests are reviewed and approved by the asset owner	TBD
e.	Standard procedures are implemented to grant and revoke access (e.g., Role-based access control)	TBD
f.	Access privileges are periodically reviewed and updated to ensure validity	TBD
g.	Least privilege and separation of duties principles are applied	TBD
h.	Access to assets is granted by the asset owner based on risk to the function	TBD
i.	Anomalous access attempts are monitored to inform situational awareness	TBD

3. Please rate your implementation of the following activities associated with planning and managing ***Identity and Access Management*** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	One or more standards and/or guidelines have been identified to inform the activities	TBD
c.	One or more policies are in place that guide the activities	TBD
d.	The policies include compliance requirements for specified standards and/or guidelines	TBD
e.	The activities are periodically reviewed to ensure conformance with the policy	TBD
f.	Stakeholders are identified and involved in the activities	TBD
g.	Resources (people, funding, and tools) are provided to support the activities	TBD
h.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

WORKFORCE Domain

Workforce Management

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.

- Responsibilities
- Workforce controls
- Knowledge, skills, and abilities
- Awareness

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **workforce cybersecurity responsibilities**.
   a. Cybersecurity responsibilities for the function are identified — TBD
   b. Cybersecurity requirements for roles are established (e.g., separation of duties, least privilege) — TBD
   c. Cybersecurity responsibilities are assigned to specific roles, including external service providers — TBD
   d. Cybersecurity responsibilities are documented in position descriptions — TBD
   e. Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate — TBD
   f. Cybersecurity responsibilities are included in job performance evaluation criteria — TBD
   g. Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage — TBD

WORKFORCE

2. Please rate your implementation of the following activities associated with managing **the workforce lifecycle**.

a. Personnel transfer and termination procedures are defined and address cybersecurity	TBD
b. Risk designations are created based on risk analysis	TBD
c. Risk designations are assigned to positions	TBD
d. Recruiting and retention are aligned to support cybersecurity workforce management objectives	TBD
e. Succession planning is performed for personnel based on risk designation	TBD
f. Security policy includes a formal disciplinary process and sanctions for employees who commit violations of security policy	TBD
g. 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	TBD
h. Personnel vetting is performed periodically for positions that have responsibilities for or access to the assets required for delivery of the function	TBD
i. Vetting is performed for employees, vendors, and contractors at a level commensurate with position risk designation	TBD

3. Please rate your implementation of the following activities associated with **cybersecurity training**.

a. Cybersecurity training is made available to personnel with cybersecurity responsibilities	TBD
b. Cybersecurity knowledge, skill, and ability gaps are identified	TBD
c. Personnel with cybersecurity responsibilities complete continuing education and professional development	TBD
d. Assessments of specific workforce skills are performed	TBD
e. Assessments of the training program are performed	TBD
f. Plan to address identified cybersecurity knowledge, skill, and ability gaps is maintained	TBD
g. Personnel with cybersecurity responsibilities complete continuing education and professional development, consistent with job role and cybersecurity responsibilities	TBD

WORKFORCE

4. Please rate your implementation of the following activities associated with **cybersecurity awareness.**

a. Cybersecurity awareness activities occur	TBD
b. Cybersecurity awareness activities occur in accordance with a defined awareness plan	TBD
c. Cybersecurity awareness content is based on understanding of function-specific cybersecurity threats	TBD
d. Cybersecurity awareness content is based on an understanding of organization-specific (cross-function) cybersecurity threats	TBD

5. Please rate your implementation of the following activities associated with planning and managing **Workforce Management activities**.

a. One or more plans or procedures are in place that guide the activities	TBD
b. One or more standards and/or guidelines have been identified to inform the activities	TBD
c. One or more policies are in place that guide the activities	TBD
d. The policies include compliance requirements for specified standards and/or guidelines	TBD
e. The activities are periodically reviewed to ensure conformance with the policy	TBD
f. Stakeholders are identified and involved in the activities	TBD
g. Resources (people, funding, and tools) are provided to support the activities	TBD
h. Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i. Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

DEPENDENCIES Domain

Supply Chain and External Dependencies Management

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.

- Dependency identification
- Risk management
- Cybersecurity requirements

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **identifying dependencies**.
   a. Important suppliers and other up-stream dependencies are identified (i.e. external parties on which the delivery of the function depend) TBD
   b. Important down-stream dependencies are identified (i.e. external parties that are dependent on the delivery of the function) TBD
   c. Important suppliers and up-stream dependencies are identified according to a defined practice TBD
   d. Important down-stream dependencies are identified according to a defined practice TBD
   e. Dependencies are prioritized based on established criteria TBD
   f. Bidirectional dependencies are identified TBD
   g. Single-source dependencies are identified TBD

2. Please rate your implementation of the following activities associated with **dependency risk management**.
   a. Significant cybersecurity risks due to suppliers and other external dependencies are identified and addressed TBD
   b. Cybersecurity risks due to suppliers and other external dependencies are identified according to a defined practice TBD
   c. Identified external dependency cybersecurity risks are analyzed and disposed according to a defined practice TBD
   d. Cybersecurity risks due to external dependencies are managed according to the organization’s risk management criteria and process TBD
   e. Suppliers, vendors, and other upstream dependencies are integrated into the information sharing process TBD

DEPENDENCIES

3. Please rate your implementation of the following activities associated with **cybersecurity requirements**.

a.	Cybersecurity requirements are considered when establishing relationships with external entities	TBD
b.	Cybersecurity requirements are established for suppliers and up-stream dependencies according to a defined practice, including requirements for secure software development practices where appropriate	TBD
c.	Agreements with suppliers and other external entities include cybersecurity requirements	TBD
d.	Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements	TBD
e.	Agreements with suppliers and other up-stream dependencies require notification of cybersecurity incidents related to the delivery of the product or service	TBD
f.	Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements	TBD
g.	Cybersecurity requirements are established for up-stream dependencies based on the organization's risk criteria	TBD
h.	Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended lifecycle of delivered products	TBD
i.	Acceptance testing of procured assets includes testing for cybersecurity specifications (Note: this should be coordinated with change management activities in *Asset, Change, and Configuration Management*)	TBD
j.	Authoritative information sources are monitored to identify and avoid known sources of counterfeit parts and services	TBD

DEPENDENCIES

4. Please rate your implementation of the following activities associated with planning and managing **Supply Chain and External Dependencies Management** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	One or more standards and/or guidelines have been identified to inform the activities	TBD
c.	One or more policies are in place that guide the activities	TBD
d.	The policies include compliance requirements for specified standards and/or guidelines	TBD
e.	The activities are periodically reviewed to ensure conformance with the policy	TBD
f.	Stakeholders are identified and involved in the activities	TBD
g.	Resources (people, funding, and tools) are provided to support the activities	TBD
h.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

THREAT Domain

Threat and Vulnerability Management

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.

- Threat management
- Vulnerability management
- Cybersecurity patch management
- Assessments

Within the function (generation, transmission, distribution, or retail) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **threat management**.
   a. Cybersecurity threat information is gathered and interpreted for the function — TBD
   b. Threats that are considered important to the function are mitigated — TBD
   c. Information sources to support threat management activities are identified and monitored (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors) — TBD
   d. Guidelines or criteria are established and used in the analysis and prioritization of identified threats — TBD
   e. Threats are addressed according to the prioritization criteria and mitigating actions are validated — TBD
   f. Threat information is shared through participation in identified information sharing channels — TBD
   g. Analysis and prioritization of threats are informed by the function's risk criteria — TBD
   h. Threat identification and analysis activities inform function's risk management activities — TBD

THREAT

2. Please rate your implementation of the following activities associated with **vulnerability management**.

a.	Cybersecurity vulnerability information is gathered and interpreted for the function	TBD
b.	Vulnerabilities that are considered important to the function are remediated	TBD
c.	Information sources to support vulnerability management activities are identified and monitored	TBD
d.	Guidelines or criteria are established and used in the analysis and prioritization of identified vulnerabilities	TBD
e.	Vulnerabilities are addressed according to the prioritization criteria and remediation actions are validated	TBD
f.	Vulnerability management activities are informed by the function's risk criteria	TBD
g.	Vulnerability identification and analysis activities inform function's risk management activities	TBD
h.	Vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)	TBD

3. Please rate your implementation of the following activities associated with **cybersecurity patch management**.

a.	Patches that mitigate cybersecurity vulnerabilities are deployed	TBD
b.	Information sources to support patch management activities are identified and monitored	TBD
c.	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)	TBD
d.	Patches are deployed according to the prioritization criteria (Note: prioritization criteria should include coverage of emergency patching)	TBD
e.	Patch management activities are informed by the function’s risk criteria	TBD

THREAT

4. Please rate your implementation of the following activities associated with planning and managing **Threat and Vulnerability Management** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	One or more standards and/or guidelines have been identified to inform the activities	TBD
c.	One or more policies are in place that guide the activities	TBD
d.	The policies include compliance requirements for specified standards and/or guidelines	TBD
e.	The activities are periodically reviewed to ensure conformance with the policy	TBD
f.	Stakeholders are identified and involved in the activities	TBD
g.	Resources (people, funding, and tools) are provided to support the activities	TBD
h.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

RESPONSE Domain

Event and Incident Response, Continuity of Operations

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.

- Detect events
- Declare incidents
- Respond to incidents
- Manage continuity

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **cybersecurity event detection**.

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 with the responsibility for receiving such reports	TBD
b.	Events are detected or reported according to a defined practice	TBD
c.	Events are logged and tracked according to a defined practice	TBD
d.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	TBD
e.	Cybersecurity event detection is informed by *Threat and Vulnerability Management* and *Risk Management* information (e.g., event detection is tuned to help detect known threats and monitor for identified risks)	TBD
f.	Cybersecurity event detection is enabled by *Situational Awareness* activities (e.g., the common operating picture for the function is monitored to support the identification of cybersecurity events)	TBD

RESPONSE

2. Please rate your implementation of the following activities associated with **cybersecurity incident declaration**.

a.	Cybersecurity incident criteria are established based on the potential impact to the function	TBD
b.	Events are analyzed to identify and declare cybersecurity incidents	TBD
c.	Events are analyzed according to a defined practice	TBD
d.	Incidents are logged and tracked to closure according to a defined practice	TBD
e.	Cybersecurity incident declaration criteria are periodically updated according to a defined practice	TBD
f.	Events are analyzed to identify and declare cybersecurity incidents according to a defined practice	TBD
g.	Declared incidents are correlated to support the discovery of patterns, trends, and other common features	TBD
h.	Incident declaration criteria are periodically updated based on *Threat and Vulnerability Management*, *Situational Awareness*, and *Risk Management* information	TBD

3. Please rate your implementation of the following activities associated with **cybersecurity incident response**.

a.	Actions are taken to respond to cybersecurity incidents to limit impact to the function and restore normal operations	TBD
b.	Incident response personnel are identified and roles are assigned	TBD
c.	Incident response is performed according defined procedures that address all phases of the incident lifecycle (e.g., triage, handling, communication, coordination, and closure)	TBD
d.	Incident response procedures are exercised	TBD
e.	Training is conducted for incident response teams	TBD
f.	Cybersecurity incident root-cause analysis and lessons-learned activities are performed as part of the defined process	TBD
g.	Procedures are followed to coordinate and collaborate with law enforcement when appropriate, including support for evidence collection and preservation	TBD
h.	Incident response personnel participate in community cybersecurity exercises (e.g., table top, simulated incidents)	TBD
i.	The incident response process is periodically reviewed and updated	TBD
j.	Incident response activities are coordinated with relevant external entities	TBD

RESPONSE

4. Please rate your implementation of the following activities associated with **continuity management**.

a.	Assets that are important to the delivery of the function are identified (Note: this may be connected to or provided from *Asset, Change, and Configuration Management*)	TBD
b.	The activities necessary to sustain minimum operations of the function are identified	TBD
c.	The sequence of activities necessary to return the function to normal operation is identified	TBD
d.	Business impact analyses are conducted according to defined practices to inform the development of continuity plans	TBD
e.	Recovery time objectives are established for the function	TBD
f.	Continuity plans are developed to sustain and restore operation of the function according to a defined practice	TBD
g.	Continuity plans are evaluated and exercised	TBD
h.	Business impact analyses are periodically reviewed and updated	TBD
i.	The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly	TBD
j.	Continuity plans are periodically reviewed and updated	TBD

5. Please rate your implementation of the following activities associated with planning and managing ***Event and Incident Response and Continuity of Operations*** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	One or more standards and/or guidelines have been identified to inform the activities	TBD
c.	One or more policies are in place that guide the activities	TBD
d.	The policies include compliance requirements for specified standards and/or guidelines	TBD
e.	The activities are periodically reviewed to ensure conformance with the policy	TBD
f.	Policy and/or procedures for reporting incident information to designated authorities conform with applicable laws, regulations, and contractual agreements	TBD
g.	Stakeholders are identified and involved in the activities	TBD
h.	Resources (people, funding, and tools) are provided to support the activities	TBD
i.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
j.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

SITUATION Domain

Situational Awareness

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.

- Logging
- Monitoring
- Awareness

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **logging**.
   a. Logging capabilities are identified and selected capabilities are activated — TBD
   b. A consistent level of logging is occurring for assets important to the function — TBD
   c. Logging requirements have been defined and documented for all assets of selected classes and/or priority — TBD
   d. Logging is performed in compliance with the documented requirements — TBD
   e. Logs are managed with consistency within the function — TBD
   f. Log data are being aggregated within the function — TBD
   g. Logging requirements are based on the risk to the function — TBD
   h. Logging is integrated with other business and security processes — TBD

SITUATION

2. Please rate your implementation of the following activities associated with **monitoring**.

a.	Cybersecurity monitoring activities are performed (e.g. periodic reviews of log data)	TBD
b.	Operational environments are monitored for anomalous behavior that may indicate a cybersecurity event	TBD
c.	Monitoring and analysis requirements have been defined and documented	TBD
d.	Monitoring and analysis is performed in compliance with the documented requirements	TBD
e.	Monitoring requirements are based on the risk to the function	TBD
f.	Monitoring is integrated with other business and security processes	TBD
g.	Alarms and alerts are implemented	TBD
h.	Alarms and alerts are defined by severity level for both power system and cybersecurity information	TBD

3. Please rate your implementation of the following activities associated with **awareness**.

a.	A local operating picture exists for the function	TBD
b.	A common operating picture exists across functions	TBD
c.	The cybersecurity operations of the function are informed based on the common operating picture	TBD
d.	Common operating picture incorporates information from external sources (including external entities on which the function depends)	TBD
e.	Pre-defined states of operation are defined and invoked (manual or automated process) based on the common operating picture	TBD

SITUATION

4. Please rate your implementation of the following activities associated with planning and managing **Situational Awareness** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	One or more standards and/or guidelines have been identified to inform the activities	TBD
c.	One or more policies are in place that guide the activities	TBD
d.	The policies include compliance requirements for specified standards and/or guidelines	TBD
e.	The activities are periodically reviewed to ensure conformance with the policy	TBD
f.	Stakeholders are identified and involved in the activities	TBD
g.	Resources (people, funding, and tools) are provided to support the activities	TBD
h.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
i.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

SHARING Domain

Information Sharing and Communications

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.

- Communication
- Analysis
- Coordination

Within the function (generation, transmission, distribution, or markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with **cybersecurity information sharing**.
   a. The key stakeholders (including connected utilities) with which information needs to be shared have been identified — TBD
   b. Communication with key stakeholders is performed — TBD
   c. Communication with key stakeholders is based on documented communication strategies within functional areas — TBD
   d. Contracts and agreements with third parties incorporate sharing of cybersecurity threat information — TBD
   e. Cybersecurity information reporting requirements are identified — TBD
   f. Information shared supports situational awareness at organization, regional, and national levels — TBD

2. Please rate your implementation of the following activities associated with **cybersecurity information analysis**.
   a. Analysis of shared information is performed — TBD
   b. Analysis of shared information occurs based on defined procedures — TBD
   c. Procedures are in place to create action plans in response to information received — TBD
   d. Technical sources are identified that can be accessed to gain expert insights — TBD
   e. Procedures are in place to analyze and de-conflict received information — TBD

3. Please rate your implementation of the following activities associated with **cybersecurity coordination**.

a.	Responsibility for the collection of shared cybersecurity information is assigned	TBD
b.	Cybersecurity information is shared across functional areas	TBD
c.	Trusted information sharing partners are identified	TBD
d.	The function participates with information sharing and analysis centers	TBD
e.	A robust network of internal and external trust relationships (both formal and informal) has been established to vet and validate information about cyber events	TBD
f.	There is a strategy or policy and procedure for incident coordination with external partners & stakeholders	TBD
g.	Provisions are established and maintained to enable secure sharing of sensitive or classified information	TBD

4. Please rate your implementation of the following activities associated with planning and managing ***Cybersecurity Information Sharing and Communications*** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	Plans for the activities address both standard operations and emergency operations	TBD
c.	One or more standards and/or guidelines have been identified to inform the activities	TBD
d.	One or more policies are in place that guide the activities	TBD
e.	The policies include compliance requirements for specified standards and/or guidelines	TBD
f.	The policies address protected information, ethical use and sharing of information, including, as appropriate, sensitive and classified information	TBD
g.	The activities are periodically reviewed to ensure conformance with the policy	TBD
h.	Stakeholders are identified and involved in the activities	TBD
i.	Resources (people, funding, and tools) are provided to support the activities	TBD
j.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
k.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

CYBER Domain

Cybersecurity Program Management

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.

- Strategy
- Sponsorship
- Program
- Architecture

Within the function (generation, transmission, distribution, markets) that is the focus of this evaluation, please answer the following questions:

1. Please rate your implementation of the following activities associated with the **cybersecurity program strategy**.
   a. The organization's strategic objectives are generally understood among senior management — TBD
   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 — TBD
   c. The organization's strategic objectives are documented and well-understood throughout the organization — TBD
   d. The organization's cybersecurity strategy and priorities are documented and aligned with the organization's strategic objectives — TBD
   e. The development and implementation of a cybersecurity strategy and its integration with organizational objectives is required by policy — TBD
   f. Cybersecurity strategy and objectives address the organization's role in critical infrastructure — TBD

2. Please rate your implementation of the following activities associated with **sponsorship of the cybersecurity program**.

a.	Some resources (people, tools, and funding) are provided to support cybersecurity activities, but may be compartmentalized (or siloed)	TBD
b.	Senior management is aware of cybersecurity concerns and provides at least vocal sponsorship for cybersecurity activities	TBD
c.	The importance and value of cybersecurity activities is regularly communicated by senior management	TBD
d.	Activities to support and develop a culture of cybersecurity in the organization are sponsored	TBD
e.	The creation and maintenance of a cybersecurity program plan is sponsored by the organization	TBD
f.	If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program	TBD
g.	Adequate funding and other resources (i.e. people and tools) are provided to establish and operate a cybersecurity program	TBD
h.	The development and maintenance of cybersecurity policies and guidelines is sponsored	TBD

3. Please rate your implementation of the following activities associated with the **cybersecurity program**.

a.	Cybersecurity activities are performed by individuals in the organization and may be compartmentalized	TBD
b.	Cybersecurity requirements are developed for key operational systems and assets	TBD
c.	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	TBD
d.	Industry activities are monitored to identify emerging cybersecurity trends, issues, standards, and initiatives	TBD
e.	Cybersecurity activities across the function and across the domains in this model are integrated, coordinated, and aligned into a systematic policy and procedure to ensure that the organization's cybersecurity objectives and strategy are addressed	TBD
f.	Organization monitors and participates in selected emerging cybersecurity standards or initiatives to support cybersecurity strategies and objectives	TBD
g.	Coordination occurs with organization's compliance efforts to support ongoing achievement of any cybersecurity compliance requirements	TBD

4. Please rate your implementation of the following activities associated with **cybersecurity architecture**.

   a. A strategy to architecturally isolate the organization's IT systems from OT systems is implemented — TBD

   b. A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy and priorities — TBD

   c. Architectural segmentation and isolation is maintained according to a documented plan — TBD

   d. Architectural segmentation and isolation strategies are informed by the organization's risk tolerance — TBD

   e. Cybersecurity architecture is routinely updated as may be required to keep it current and to address new requirements — TBD

5. Please rate your implementation of the following activities associated with **cybersecurity requirements for software development** (including software developed internally and software developed by third parties).

   a. Software to be deployed on assets of selected classes and/or priority is developed using secure software development practices — TBD

   b. Policies require that software to be deployed on assets above a priority threshold be developed using secure software development practices — TBD

6. Please rate your implementation of the following activities associated with planning and managing ***Cybersecurity Program*** activities.

a.	One or more plans or procedures are in place that guide the activities	TBD
b.	Question deleted	
c.	One or more standards and/or guidelines have been identified to inform the activities	TBD
d.	One or more policies are in place that guide the activities	TBD
e.	The policies include compliance requirements for specified standards and/or guidelines	TBD
f.	The policies include compliance requirements for any applicable regulations related to cybersecurity	TBD
g.	Question deleted	
h.	The activities are periodically reviewed to ensure conformance with the policy	TBD
i.	Stakeholders are identified and involved in the activities	TBD
j.	Responsibility and authority for the performance of the activities are assigned to personnel	TBD
k.	Personnel performing the activities have the skills and knowledge needed to perform their assigned responsibilities	TBD

7. Please rate your implementation of the following cross-domain activities.

a.	Asset inventory attributes support *Threat and Vulnerability Management* (i.e., inventory includes sufficient information about the assets to enable threat and vulnerability analysis)	TBD
b.	Configuration management [ASSET] is coordinated with cybersecurity patch management [THREAT] (i.e., configuration baselines are updated to reflect the deployment of patches to mitigate cybersecurity vulnerabilities)	TBD
c.	Change management activities are coordinated with *Threat and Vulnerability Management* activities (e.g., changes made to mitigate vulnerabilities are subject to the change management procedures)	TBD
d.	*Asset, Change, and Configuration Management* activities are coordinated with *Supply Chain and External Dependencies Management* activities for high priority assets that are dependent on external parties (i.e., the performance of asset inventory, change management, and configuration management activities for assets that are controlled by third parties are addressed in the formal agreements and requirements for the third party)	TBD
e.	Risk assessment and disposition activities [RISK] are integrated with threat and vulnerability identification and assessment [THREAT]	TBD
f.	Threat and vulnerability management information [THREAT] is communicated within the function to support situational awareness activities [SITUATION]	TBD
g.	*Event and Incident Response, Continuity of Operations* Incident response information [RESPONSE] is shared with relevant external entities (e.g., ES-ISAC, trade associations, vendors) [SHARING][DEPENDENCIES]	TBD
h.	Response and continuity activities [RESPONSE] are coordinated with *Asset, Change, and Configuration Management* activities to ensure that restored assets are configured appropriately and inventory information is updated	TBD
i.	Common operating picture is shared with stakeholders external to the function [SHARING][DEPENDENCIES]	TBD

Glossary

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

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 operations 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

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 (e.g., personnel, contractor) is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity (e.g., personnel, contractor).	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 (e.g., personnel, contractor) 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