UCF Mapping Report

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 Draft 2

Disclaimer

This Authority Document In Depth Report provides analysis and guidance for use and implementation of the Authority Document but it is not a substitute for the original authority document itself. Readers should refer to the original authority document as the definitive resource on obligations and compliance requirements.

Authority Document Catalog Information

US National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 Draft 2*, issued by National Institute of Standards and Technology

This is a International or National Standard and is mapped as UCF Authority Document ID 0002900 as a part of the North America category. Its primary subject matter is CyberSecurity.

This document's original availability is Free. It was accessed online December 10, 2017 at: https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf

The process we used to tag and map this document

This document has been mapped into the Unified Compliance Framework using a patented methodology and patented tools (you can research our patents HERE). The mapping team has taken every effort to ensure the quality of mapping is of the highest degree. To learn more about the process we use to map Authority Documents, or to become involved in that process, click HERE.

What is presented below is a series of Citations and their Mandates abstracted from the original document. This is not meant as a replacement for the original document (which can be obtained from the link provided below) – it is provided as a scientific analysis of the document, analyzing its mandates based on their breakdowns into primary and secondary verbs and nouns.

Analysis

The analysis of this document is broken down into four parts; Common Controls by Impact Zone, Term and Mandate Summary, Mandate Tagging Analysis, Suggested Glossary

Common Controls by Impact Zone

An Impact Zone is a hierarchical way of organizing our suite of Common Controls — it is a taxonomy. The top levels of the UCF hierarchy are called Impact Zones. Common Controls are mapped within the UCF’s Impact Zones and are maintained in a legal hierarchy within that Impact Zone. Each Impact Zone deals with a separate area of policies, standards, and procedures: technology acquisition, physical security, continuity, records management, etc.

Common Controls by Impact Zone	**134 Mandated** *90 Implied* 1735 Implementation
Audits and risk management	**130**
Human Resources management	**81**
Leadership and high level objectives	**111**
Monitoring and measurement	**151**
Operational and Systems Continuity	**88**
Operational management	**317**
Physical and environmental protection	**197**
Privacy protection for information and data	**23**
Records management	**107**
System hardening through configuration management	**481**
Systems design, build, and implementation	**30**
Technical security	**212**
Third Party and supply chain oversight	**31**

The UCF created its taxonomy by looking at the corpus of standards and regulations through the lens of unification and a view toward *how the controls impact the organization*. Thus, we created a hierarchical structure for each impact zone that takes into account regulatory and standards bodies, doctrines, and language.

Term and Mandate Summary

This Authority Document has 176 citations mapped to 134 UCF Common Control IDs.

Percent (%) of Citations with multiple mandates: 22.8% Multiple Mandates in a Citation happens when the Authority Document author tells you to do this, that, and the other all in the same sentence or paragraph. If you have to perform multiple, distinct tasks, each of those is a Mandate in and of itself. The UCF breaks down these types of Citations into individual Mandates so that you know what you really should be doing. The more Citations with multiple Mandates, the harder the document is to follow.

Percent (%) of terms mapped into the AD's glossary: 7.1% Primary verbs and nouns *not mapped into an AD's glossary* can point to the AD's authors not paying attention to the definitions of their terms.

Percent (%) of terms where fewer than 5 other ADs referenced the term: 15.8% Any term in this category is not very widely used by the rest of the compliance community and therefore will more than likely need to be further investigated for any implications it might bring.

Percent (%) of mandates where only 1 to 5 other ADs mapped to the Common Control: 13.1% Mandates that aren't widely called for will take longer to implement than mandates that are more familiar.

Number of mandates where 0 other ADs mapped to the Common Control: 15.9% These mandates are *only called for by this AD*, making them particularly thorny to implement, as this AD is the "lone wolf" in asking for them to be followed.

Citation and Mandate Tagging and Mapping

Most Authority Documents have both mandates and explanatory text. They will say "Go do this" (which is the mandate) and then sometimes explain what "this" is, or give references, or add additional information about how they want "this" done. The UCF mapping process focusses on the mandates and ignores any explanatory text or other information found within a Citation.

If a Citation has multiple mandates, for example, "Turn off the lights then lock the door.", in order to disambiguate the mandates as against the Common Controls we will tag ***each and every mandate separately***. The Citation will be listed multiple times, once for each mandate found within the Citation. This is imperative to the mapping process, because only one mandate at a time can be mapped to a Common Control.

What follows is a listing of each Citation we found within Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 Draft 2. Each Citation has been tagged with its primary and secondary nouns and primary and secondary verbs. The first column shows the Citation reference (the section number or other marker within the Authority Document that points to where we found the guidance). The second column shows the Citation guidance per se, along with the tagging for the mandate we found within the Citation. The third column shows the Common Control ID to which the mandate has been mapped, and the final column provides the Common Control itself.

Citations with no tagging, no CC ID, and no associated Control Title are known as "Stub" Citations. Stub Citations are partial sentences or citations with no mandate to do anything.

Some Citations have terms surrounded by curly brackets { }. These terms are not part of the original Citation but provide missing language that gives the Citation context required to make it mappable and understandable to our cognitive learning system.

Questions encountered during mapping

Here is the table of Citations wherein we were not sure of what was being asked, we felt the terms could be made more explicit, etc.

KEY: Primary Verb Primary Noun Secondary Verb Secondary Noun Limiting Term

CITATION REFERENCE	CITATION GUIDANCE	QUESTION/ANALYSIS/ISSUE
PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	What do you mean by *network integrity*? Physical integrity of the systems? Access Control integrity? Integrity of the network's design? Integrity meaning there are not rogue devices?
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions when appropriate	How do you *bind* someone's identity? Are you stating that the organization should *bind* the identity to the person's credentials? If so, what methodology are you talking about, and what type of credentials are you talking about?
PR.PT-5	Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations)	This is a statement. If you were to turn this into a directive, what would you be asking the users? To *audit* whether the systems are functioning in the pre-defined state versus operating out-of-band from any standardized norm?
DE.AE-4	Impact of events is determined	Impact to *what*? Impact to the organization's operations? Impact to the system's operations? Impact to privacy? Impact to the entire industry sector?
RS.AN-2	The impact of the incident is understood	Is this a follow-on do DE.AE-4? First, understand the event, then understand the incident as a whole?

Mapping to Common Controls

Here is the table of Citations as mapped to the Unified Compliance Framework. As stated earlier, the terms were tagged using an Advanced Semantic tagging system that implements Named Entity Recognition, tying the terms to various Natural Language Processing Engines to determine the primary and secondary verbs and nouns. From there, Erdös distance vectors were used to match each Citation's mandates to a Common Control. NIST may use these Mandate to Common Control Mappings in any publication or any other manner it wishes as long as the Common Control IDs are linked with each Common Control title.

KEY: Primary Verb Primary Noun Secondary Verb Secondary Noun Limiting Term

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
ID	IDENTIFY		
ID.AM Asset Management ✓ Multiple Mandates	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	00689	Establish and maintain an Information Technology inventory with asset discovery audit trails.
ID.AM Asset Management ✓ Multiple Mandates	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	06630	Establish and maintain an Asset Management program.
ID.AM-1	Physical devices and systems within the organization are inventoried	00689	Establish and maintain an Information Technology inventory with asset discovery audit trails.
ID.AM-2	Software platforms and applications within the organization are inventoried	00692	Include software in the Information Technology inventory.
ID.AM-3	Organizational communication and data flows are mapped.	10059	Maintain up-to-date data flow diagrams.
ID.AM-4	External information systems are catalogued	04885	Include interconnected systems and Software as a Service in the Information Technology inventory.
ID.AM-5	Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their	07186	Classify assets according to the Asset Classification Policy.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
	classification, criticality, and business value		
ID.AM-6 ✓ 0 other ADs match the Control	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	13201	Establish and maintain cybersecurity roles and responsibilities.
ID.BE Business Environment ✓ Multiple Mandates	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	00598	Analyze organizational objectives, functions, and activities.
ID.BE Business Environment ✓ Multiple Mandates	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	11750	Define and assign the security staff roles and responsibilities.
ID.BE Business Environment ✓ Multiple Mandates	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	00706	Establish a risk acceptance level that is appropriate to the organization's risk appetite.
ID.BE-1 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	The organization's role in the supply chain is identified and communicated	09958	Document the organization's supply chain in the supply chain management program.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
ID.BE-1 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	The organization's role in the supply chain is identified and communicated	08924	Distribute collected supply chain information to purchasers.
ID.BE-2 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	The organization's place in critical infrastructure and its industry sector is identified and communicated	12798	Analyze the business environment in which the organization operates.
ID.BE-2 ✓ 0 other ADs match the Control ✓ Multiple Mandates	The organization's place in critical infrastructure and its industry sector is identified and communicated	13200	Communicate the organization's business environment and place in its industry sector, as necessary.
ID.BE-3 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	Priorities for organizational mission, objectives, and activities are established and communicated	09960	Prioritize organizational objectives.
ID.BE-3 ✓ 0 other ADs match the Control ✓ Multiple Mandates	Priorities for organizational mission, objectives, and activities are established and communicated	13191	Communicate organizational objectives to all interested personnel and affected parties.
ID.BE-4 ✓ 0 other ADs match the Control	Dependencies and critical functions for delivery of critical services are established	08900	Document supply chain dependencies for delivering critical services or critical functions in the supply chain management program.
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	00732	Establish and maintain a continuity framework.
ID.GV Governance	The policies, procedures, and processes to manage and monitor	12378	Include risk management in the information security program.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
	the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.		
ID.GV-1	Organizational information security policy is established	11740	Establish and maintain an information security policy.
ID.GV-2 ✓ 1-5 ADs match the Control	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	12304	Document the roles and responsibilities for all activities that protect restricted data in the information security procedures.
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	07113	Establish and maintain a list of compliance documents.
ID.GV-4 ✓ 0 other ADs match the Control	Governance and risk management processes address cybersecurity risks	13193	Address cybersecurity risks in the risk assessment program.
ID.RA Risk Assessment ✓ 1-5 ADs match the Control	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	12281	Document cybersecurity risks.
ID.RA-1	Asset vulnerabilities are identified and documented	00700	Include security vulnerabilities based upon threats to the system in the threat and risk classification scheme.
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	06489	Include security information sharing procedures in the internal control framework.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
ID.RA-3	Threats, both internal and external, are identified and documented	00699	Include security threats and hazards to the system in the threat and risk classification scheme.
ID.RA-4	Potential business impacts and likelihoods are identified	06463	Assess the potential level of business impact risk associated with each business process.
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	00703	Establish and maintain a Risk Scoping and Measurement Definitions Document.
ID.RA-6 ✓ 0 other ADs match the Control ✓ Multiple Mandates	Risk responses are identified and prioritized	13195	Include risk responses in the risk management program.
ID.RA-6 ✓ 0 other ADs match the Control ✓ Multiple Mandates	Risk responses are identified and prioritized	13195	Include risk responses in the risk management program.
ID.RM Risk Management Strategy ✓ 1-5 ADs match the Control ✓ Multiple Mandates	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	11991	Establish and Maintain a Cybersecurity Risk Management Strategy.
ID.RM Risk Management Strategy ✓ Multiple Mandates	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	00706	Establish a risk acceptance level that is appropriate to the organization's risk appetite.
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	12051	Establish and maintain a risk management program.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	00706	Establish a risk acceptance level that is appropriate to the organization's risk appetite.
ID.RM-3 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	09962	Align organizational risk tolerance to that of industry peers in the risk register.
ID.RM-3 ✓ Multiple Mandates	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	00706	Establish a risk acceptance level that is appropriate to the organization's risk appetite.
ID.SC Supply Chain Risk Management ✓ 1-5 ADs match the Control ✓ Multiple Mandates	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	12798	Analyze the business environment in which the organization operates.
ID.SC Supply Chain Risk Management ✓ Multiple Mandates	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	00706	Establish a risk acceptance level that is appropriate to the organization's risk appetite.
ID.SC Supply Chain Risk Management ✓ 0 other ADs match the	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions	13190	Include supply chain risk management procedures in the risk management program.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
Control ✔ Multiple Mandates	associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.		
ID.SC-1 ✔ 0 other ADs match the Control ✔ Multiple Mandates	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	13190	Include supply chain risk management procedures in the risk management program.
ID.SC-1 ✔ 0 other ADs match the Control ✔ Multiple Mandates	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	13198	Analyze supply chain risk management procedures, as necessary.
ID.SC-1 ✔ 0 other ADs match the Control ✔ Multiple Mandates	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	13199	Assign key stakeholders to review and approve supply chain risk management procedures.
ID.SC-2	include Identify, prioritize and assess suppliers and third-party partners of information systems, components and services using a cyber supply chain risk assessment process	06454	Perform a risk assessment prior to engaging a third party.
ID.SC-3	{Include, third party contract} Suppliers and third-party partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.	00359	Require third party security requirements to comply with the organizational security requirements.
ID.SC-4 ✔ 1-5 ADs match the	Suppliers and third-party partners are routinely assessed to confirm that they are meeting their contractual	13142	Assess the effectiveness of Third Parties' services provided to the organization.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
Control ✓ Multiple Mandates	obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted		
ID.SC-4 ✓ Multiple Mandates	Suppliers and third-party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted	04726	Monitor personnel and third parties for compliance to the organizational compliance framework.
ID.SC-5 ✓ 1-5 ADs match the Control	Response and recovery planning and testing are conducted with suppliers and third-party providers	12769	Include the coordination and interfaces among third parties in the coverage of the scope of testing the continuity plan.
PR	PROTECT		
PR.AC Identity Management, Authentication and Access Control ✓ Multiple Mandates	{access control, physical access control} Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	04553	Enable access control for objects and users on each system.
PR.AC Identity Management, Authentication and Access Control ✓ Multiple Mandates	{access control, physical access control} Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access	04553	Enable access control for objects and users on each system.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
	to authorized activities and transactions.		
PR.AC Identity Management, Authentication and Access Control ✓ Multiple Mandates	{access control, physical access control} Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	01640	Secure physical entry points with physical access controls or security guards.
PR.AC Identity Management, Authentication and Access Control ✓ 1-5 ADs match the Control ✓ Multiple Mandates	{access control, physical access control} Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	12386	Include access control in the information security program.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	00513	Establish and maintain an access rights management plan.
PR.AC-2	Physical access to assets is managed and protected	00711	Establish and maintain a facility physical security program.
PR.AC-3	Remote access is managed	00559	Control all methods of remote access and teleworking.
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	01411	Establish access rights based on least privilege.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
PR.AC-5 ✓ Multiple Mandates	Network integrity is protected, incorporating network segregation where appropriate	00529	Identify and control all network access controls.
PR.AC-5 ✓ Multiple Mandates	Network integrity is protected, incorporating network segregation where appropriate	11821	Employ firewalls to secure network connections between trusted networks and untrusted networks, as necessary.
PR.AC-6 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	Identities are proofed and bound to credentials and asserted in interactions when appropriate	12081	Identify information system users.
PR.AC-6 ✓ Multiple Mandates	Identities are proofed and bound to credentials and asserted in interactions when appropriate	00515	Control the addition and modification of user identifiers, user credentials, or other object identifiers.
PR.AC-6 ✓ 0 other ADs match the Control ✓ Multiple Mandates	Identities are proofed and bound to credentials and asserted in interactions when appropriate	13203	Validate transactions using identifiers and credentials.
PR.AC-7	{assign, authentication mechanism} Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	06856	Assign authentication mechanisms for user account authentication.
PR.AT Awareness and Training	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with	11746	Establish and maintain a security awareness program.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
	related policies, procedures, and agreements.		
PR.AT-1	All users are informed and trained	00785	Train all personnel and third parties, as necessary.
PR.AT-2 ✓ 0 other ADs match the Control	Privileged users understand roles and responsibilities	13192	Conduct bespoke roles and responsibilities training, as necessary.
PR.AT-3 ✓ 0 other ADs match the Control	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	13192	Conduct bespoke roles and responsibilities training, as necessary.
PR.AT-4 ✓ 0 other ADs match the Control	Senior executives understand roles and responsibilities	13192	Conduct bespoke roles and responsibilities training, as necessary.
PR.AT-5 ✓ 0 other ADs match the Control	Physical and information security personnel understand roles and responsibilities	13192	Conduct bespoke roles and responsibilities training, as necessary.
PR.DS Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	11619	Establish and maintain records management procedures used to manage organizational records.
PR.DS-1 ✓ 0 other ADs match the Control	Data-at-rest is protected	13204	Establish and maintain electronic storage media security controls.
PR.DS-2	Data-in-transit is protected	00564	Use strong data encryption to transmit restricted data or restricted information over public networks.
PR.DS-3 ✓ 1-5 ADs match the	{dispose of} Assets are formally managed throughout removal, transfers, and disposition	06698	Transfer legal ownership of assets when the system is redeployed to a third party.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
Control ✓ Multiple Mandates			
PR.DS-3 ✓ Multiple Mandates	{dispose of} Assets are formally managed throughout removal, transfers, and disposition	06278	Dispose of hardware and software at their life cycle end.
PR.DS-4	Adequate capacity to ensure availability is maintained	06754	Provide excess capacity or redundancy to limit any effects of a Denial of Service attack.
PR.DS-5	Protections against data leaks are implemented	00356	Limit data leakage.
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	01205	Implement file integrity monitoring.
PR.DS-7	{development environment} The development and testing environment(s) are separate from the production environment	06088	Separate the design and development environment from the production environment.
PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity	01906	Establish and maintain the systems' integrity level.
PR.IP Information Protection Processes and Procedures	{information security process, information security procedure} Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	00812	Establish and maintain an information security program.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)	02130	Create a Configuration Baseline Documentation Record before promoting the system to a production environment.
PR.IP-2	A System Development Life Cycle to manage systems is implemented	12079	Establish and maintain System Development Life Cycle documentation.
PR.IP-3	{establish and maintain} Configuration change control processes are in place	00886	Establish and maintain a change control program.
PR.IP-4 ✓ Multiple Mandates	Backups of information are conducted, maintained, and tested periodically	11692	Perform backup procedures for in scope systems.
PR.IP-4 ✓ Multiple Mandates	Backups of information are conducted, maintained, and tested periodically	01401	Test backup media for media integrity and information integrity, as necessary.
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	00724	Establish and maintain an environmental control program.
PR.IP-6	Data is destroyed according to policy	06621	Remove and/or destroy records according to the records' retention event and retention period schedule.
PR.IP-7	Protection processes are continuously improved	01348	Review the internal control framework, as necessary.
PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties	11732	Share relevant security information with Special Interest Groups, as necessary.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
PR.IP-9 ✓ Multiple Mandates	{establish and maintain} Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	12056	Establish and maintain an incident response plan.
PR.IP-9 ✓ Multiple Mandates	{establish and maintain} Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	00752	Establish and maintain a continuity plan and associated continuity procedures.
PR.IP-10 ✓ Multiple Mandates	{response plan} Response and recovery plans are tested	01216	Test the incident response procedures.
PR.IP-10 ✓ Multiple Mandates	{response plan} Response and recovery plans are tested	00755	Test the continuity plan, as necessary.
PR.IP-11 ✓ 1-5 ADs match the Control	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	10628	Establish and maintain a personnel security program.
PR.IP-12	A vulnerability management plan is developed and implemented	11636	Establish and maintain a vulnerability assessment program.
PR.MA Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	01435	Perform periodic maintenance according to organizational standards.
PR.MA-1 ✓ Multiple Mandates	Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools	01435	Perform periodic maintenance according to organizational standards.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
PR.MA-1 ✓ Multiple Mandates	Maintenance and repair of organizational assets are performed and logged in a timely manner, with approved and controlled tools	00892	Document periodic maintenance in maintenance reports.
PR.MA-2 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	10615	Approve all remote maintenance sessions.
PR.MA-2 ✓ Multiple Mandates	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	01434	Conduct maintenance with authorized personnel.
PR.MA-2 ✓ 0 other ADs match the Control ✓ Multiple Mandates	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	13202	Log the performance of all remote maintenance.
PR.PT Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	00812	Establish and maintain an information security program.
PR.PT-1 ✓ Multiple Mandates	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	00637	Establish and maintain logging and monitoring operations.
PR.PT-1 ✓ Multiple Mandates	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	00596	Review event logs, Intrusion Detection System reports, security incident tracking reports, and other security logs regularly.
PR.PT-2 ✓ Multiple Mandates	Removable media is protected and its use restricted according to policy	06680	Establish and maintain removable storage media controls.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
PR.PT-2 ✓ Multiple Mandates	Removable media is protected and its use restricted according to policy	04889	Control access to restricted storage media.
PR.PT-3 ✓ 0 other ADs match the Control	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	07599	Configure Least Functionality and Least Privilege settings in accordance with organizational standards.
PR.PT-4	Communications and control networks are protected	00529	Identify and control all network access controls.
PR.PT-5	Systems operate in pre-defined functional states to achieve availability (e.g. under duress, under attack, during recovery, normal operations)		
DE	DETECT		
DE.AE Anomalies and Events ✓ Multiple Mandates	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	00585	Monitor systems for inappropriate usage and other security violations.
DE.AE Anomalies and Events ✓ Multiple Mandates	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	01650	Determine the incident severity level when assessing the security incidents.
DE.AE-1 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	A baseline of network operations and expected data flows for users and systems is established and managed	13188	Establish and maintain a network activity baseline.
DE.AE-1 ✓ Multiple Mandates	A baseline of network operations and expected data flows for users and systems is established and managed	04542	Establish and maintain information flow procedures.
DE.AE-2	Detected events are analyzed to understand attack targets and methods	00596	Review event logs, Intrusion Detection System reports, security

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
			incident tracking reports, and other security logs regularly.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	01424	Compile the event logs of multiple components into a system-wide time-correlated audit trail.
DE.AE-4	Impact of events is determined	01650	Determine the incident severity level when assessing the security incidents.
DE.AE-5 ✓ 0 other ADs match the Control	Incident alert thresholds are established	13205	Include incident alert thresholds in the continuous security warning monitoring procedures.
DE.CM Security Continuous Monitoring ✓ Multiple Mandates	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	00637	Establish and maintain logging and monitoring operations.
DE.CM Security Continuous Monitoring ✓ 0 other ADs match the Control ✓ Multiple Mandates	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	13206	Identify cybersecurity events in event logs and audit logs.
DE.CM Security Continuous Monitoring ✓ 0 other ADs match the Control ✓ Multiple Mandates	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	13207	Correlate log entries to security controls to verify the security control's effectiveness.
DE.CM-1	The network is monitored to detect potential cybersecurity events	00585	Monitor systems for inappropriate usage and other security violations.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	00724	Establish and maintain an environmental control program.
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	04726	Monitor personnel and third parties for compliance to the organizational compliance framework.
DE.CM-4	Malicious code is detected	07072	Log and react to all malicious code activity.
DE.CM-5	Unauthorized mobile code is detected	10034	Monitor systems for unauthorized mobile code.
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	00799	Monitor third parties for performance and effectiveness, as necessary.
DE.CM-7 ✓ Multiple Mandates	{unapproved Information Technology resource} Monitoring for unauthorized personnel, connections, devices, and software is performed	06797	Monitor for unauthorized physical access at physical entry points.
DE.CM-7 ✓ Multiple Mandates	{unapproved Information Technology resource} Monitoring for unauthorized personnel, connections, devices, and software is performed	00536	Scan organizational networks for rogue devices.
DE.CM-8	Vulnerability scans are performed	11637	Perform vulnerability scans, as necessary.
DE.DP Detection Processes ✓ Multiple Mandates	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	01207	Include incident monitoring procedures in the Incident Management program.
DE.DP Detection Processes ✓ 0 other ADs match the	Detection processes and procedures are maintained and tested to ensure	13194	Test incident monitoring procedures.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
Control ✓ Multiple Mandates	timely and adequate awareness of anomalous events.		
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	01652	Include the incident response team member's roles and responsibilities in the Incident Response program.
DE.DP-2 ✓ 1-5 ADs match the Control	Detection activities comply with all applicable requirements	10035	Protect each person's right to privacy and civil liberties during intrusion management operations.
DE.DP-3 ✓ 0 other ADs match the Control	Detection processes are tested	13194	Test incident monitoring procedures.
DE.DP-4: ✓ 1-5 ADs match the Control	Event detection information is communicated to appropriate parties	12406	Establish and maintain alert procedures that follow the organization's communication protocol.
DE.DP-5	Detection processes are continuously improved	04653	Update the intrusion detection capabilities and the incident response capabilities regularly.
RS	RESPOND		
RS.RP Response Planning	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity incidents.	06942	Respond to and triage when a security incident is detected.
RS.RP-1	Response plan is executed during or after an incident	06942	Respond to and triage when a security incident is detected.
RS.CO Communications ✓ 0 other ADs match the Control ✓ Multiple Mandates	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	13196	Coordinate incident response activities with interested personnel and affected parties.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
RS.CO Communications ✓ 0 other ADs match the Control ✓ Multiple Mandates	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	13197	Include support from law enforcement authorities when conducting incident response activities, as necessary.
RS.CO-1	Personnel know their roles and order of operations when a response is needed	01652	Include the incident response team member's roles and responsibilities in the Incident Response program.
RS.CO-2	Incidents are reported consistent with established criteria	01212	Share incident information with interested personnel and affected parties.
RS.CO-3	Information is shared consistent with response plans	01212	Share incident information with interested personnel and affected parties.
RS.CO-4 ✓ 0 other ADs match the Control	{coordinate} Coordination with stakeholders occurs consistent with response plans	13196	Coordinate incident response activities with interested personnel and affected parties.
RS.CO-5	{share} Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	01212	Share incident information with interested personnel and affected parties.
RS.AN Analysis ✓ 1-5 ADs match the Control	{analyze} Analysis is conducted to ensure adequate response and support recovery activities.	13179	Analyze the incident response process following an incident response.
RS.AN-1	Notifications from detection systems are investigated	06434	Respond to all alerts from security systems in a timely manner.
RS.AN-2	The impact of the incident is understood	00701	Analyze and quantify the risks to in scope systems and information.
RS.AN-3	Forensics are performed	02236	Collect evidence from the incident scene.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
RS.AN-4 ✓ 0 other ADs match the Control	Incidents are categorized consistent with response plans	13208	Categorize the incident following an incident response.
RS.AN-5	{establish and maintain, threat and vulnerability management process} Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	00687	Establish and maintain a risk assessment program to manage internal threats and external threats.
RS.MI Mitigation ✓ Multiple Mandates	{incident containment process, incident management process} Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	01751	Contain the incident to prevent further loss and preserve the system for forensic analysis.
RS.MI Mitigation ✓ Multiple Mandates	{incident containment process, incident management process} Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	01757	Eradicate the cause of the security incident after the security incident has been contained.
RS.MI-1	Incidents are contained	01751	Contain the incident to prevent further loss and preserve the system for forensic analysis.
RS.MI-2 ✓ 1-5 ADs match the Control	Incidents are mitigated	12973	Mitigate reported incidents.
RS.MI-3 ✓ Multiple Mandates	Newly identified vulnerabilities are mitigated or documented as accepted risks	11940	Rank discovered vulnerabilities.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
RS.MI-3 ✓ 1-5 ADs match the Control ✓ Multiple Mandates	Newly identified vulnerabilities are mitigated or documented as accepted risks	12973	Mitigate reported incidents.
RS.MI-3 ✓ Multiple Mandates	Newly identified vulnerabilities are mitigated or documented as accepted risks	00706	Establish a risk acceptance level that is appropriate to the organization's risk appetite.
RS.IM Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	01234	Include lessons learned from analyzing security violations in the Incident Management program.
RS.IM-1	Response plans incorporate lessons learned	01234	Include lessons learned from analyzing security violations in the Incident Management program.
RS.IM-2	Response strategies are updated	00754	Review and update the continuity plan.
RC	RECOVER		
RC.RP Recovery Planning ✓ 1-5 ADs match the Control	Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity incidents.	10604	Implement the continuity plan, as necessary.
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident	01373	Activate the continuity plan if the damage assessment report indicates the activation criterion has been met.
RC.IM Improvements ✓ Multiple Mandates	{recovery process} Recovery planning and processes are improved by incorporating lessons learned into future activities.	10037	Document and use the lessons learned to update the continuity plan.

CITATION REFERENCE	CITATION GUIDANCE	CC ID	COMMON CONTROL TITLE
RC.IM Improvements ✓ Multiple Mandates	{recovery process} Recovery planning and processes are improved by incorporating lessons learned into future activities.	10037	Document and use the lessons learned to update the continuity plan.
RC.IM-1	Recovery plans incorporate lessons learned	10037	Document and use the lessons learned to update the continuity plan.
RC.IM-2	Recovery strategies are updated	00754	Review and update the continuity plan.
RC.CO Communications	{interested personnel, affected party} Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	01386	Coordinate continuity planning with other business units responsible for related continuity plans.
RC.CO-1	Public relations are managed	01759	Share data loss event information with the media.
RC.CO-2	Reputation after an event is repaired	01759	Share data loss event information with the media.
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams	01212	Share incident information with interested personnel and affected parties.

Suggested Glossary

The following terms are both verbs and nouns that were mapped within your document. We highly suggest that you draw from this suggested glossary and add it to the final glossary. All terms and definitions are found within ComplianceDictionary.com. If you use the terms in the glossary, you are free to do so as long as ComplianceDictionary.com is referenced.

TERM	DEFINITION	DEFINED WITHIN
accept	To consent to receive (something given or offered).	
access control	A system or measures that limit the retrieving, obtaining, or examining of information, or information processing resources, to persons or applications authorized by the system or data classification.	
access right	Authorization to gain access to something physically or logically.	
accord	Harmony of people's opinions or actions or characters.	
activity	Activities are the major tasks performed by the organization to accomplish each of its functions. Activities are usually defined as part of processes or plans, and are documented in procedures. Several activities may be associated with each function. An activity is identified by the name it is given and its scope (or definition). The scope of the activity encompasses all of the transactions that take place in relation to it. Depending on the nature of the transactions involved, an activity may be performed in relation to one function, or it may be performed in relation to many functions. In cost accounting, an activity is the actual work task or step performed in producing and delivering products and services. An aggregation of activities performed within an organization that is useful for purposes of activity-based costing.	
address	To deal with an issue.	
affected party	This role is focused on contracting parties who are affected by organizational activities. Any individual who is in a contract and is affected by organizational activities should be assigned to this role.	
after	This limits a Control or Mandate's secondary verb to be put into play once the event taking place has concluded.	
agree	Be in accord; be in agreement.	
agreement	This record category contains records of mutual understandings, written or verbal, made by two or more parties regarding a matter of opinion or their rights and obligations toward each other.	
align	To give support to; come together in agreement or alliance.	
analyze	To examine methodically, typically for purposes of explanation and interpretation.	
anomalous activity	Any actions that are outside of what is expected, as measured against what "normally" should be happening, occur.	
applicable requirement	The relevant or appropriate necessary condition or conditions.	
application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements. An application contrasts with systems program, such as an operating system or network control program, and with utility programs, such as copy or sort.	

TERM	DEFINITION	DEFINED WITHIN
approve	Give sanction to.	
assert	To state as having existence; affirm; postulate.	
assess	To estimate or determine the nature, value, ability, or quality of someone or something; evaluate.	
assessed risk	A detected and evaluated risk. An assessed risk of material misstatement at the assertion level is a significant risk.	
asset	Anything of material value or usefulness that is owned by a person or company.	
asset vulnerability	A weakness in any of the organization's property of material value or usefulness or physical layout that could be accidentally triggered or intentionally exploited by a threat in order to gain unauthorized access to information or disrupt processing.	
assign	To appoint someone to a job, duty, task, or organization; allocate a job, duty, or task.	
assumption	Something that is accepted as true without proof.	
audit	A systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.	
audit log	A security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.	
authentication mechanism	Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system.	
authorized device	A computer device that the organization has authorized to be used and connected to the system.	
authorized user	A person who has the authority or permission to manage access or make changes to an account.	
backup	A copy of files, data, or programs that is generally used for restoration in the event of damage or loss to the original files, data, or programs.	
base	To serve as a foundation, underlying support, or starting point for something.	
baseline configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.	
bind	The process of associating two related elements of information.	
business continuity testing	The act of performing a test to evaluate the effectiveness of an organization's business continuity plan.	

TERM	DEFINITION	DEFINED WITHIN
business impact	The financial, reputational or operational consequences to the business.	
Business Value	How much a business is worth. Business value is a highly subjective measure because it involves estimating the value of intangible assets like trade secrets and brand recognition. It adds to this the value of tangible assets like machinery and stockholder equity. Business value is especially important for potential investors or buyers.	
buyer	A buyer is any person or organization who contracts to acquire an asset or service in return for some form of consideration.	✓
capacity	The maximum amount that something can contain.	
catalog	The process of providing such access, plus additional work to prepare the materials for use, such as labeling, marking, and maintenance of authority files.	
categorize	To arrange or place in a particular class or group.	
classification	The act of distributing things into classes or categories of the same type.	
communicate	To share or convey knowledge, information, news, or ideas.	
communication	A letter or message containing information or news.	
comply	To act in accordance with a wish, command, law, standard, or contractual obligation.	
conduct	To manage, control, or organize and carry out.	
configuration change control process	An action that is taken or performed to systematically manage all changes made to an asset's arrangement, system configuration, or security configuration in order to prevent unnecessary disruptions, vulnerabilities, and mitigate threats. Its purpose is to ensure that all changes to a complex system are performed with the knowledge and consent of management.	
configure a system	The setting of various switches and jumpers for hardware and the defining of values of parameters for software. Each parameter specifies a preferred or required setting or policy for a computer system, or a configuration control such as a particular registry key, file, or GPO setting. Every parameter includes descriptive elements in a human-understandable manner.	
confirm	Establish the truth or correctness of something previously believed to be the case.	
constraint	The state of being restricted or prevented.	
contain	To have, hold, include, or be a part of.	
continuity requirement	A statement of a necessary condition to provide continuity.	
contractual obligation	A course of action or conditions that someone is legally bound to because they signed a contract.	

TERM	DEFINITION	DEFINED WITHIN
control	To exercise authority over; direct; regulate. This include exercising authority over the processesses of issuance and revocation, management, and auditing.	
coordinate	To bring the different elements of a complex activity into a relationship that will ensure efficiency.	
correlate	To have or establish a mutual connection or relationship, in which one thing affects or depends on another.	
create and maintain	Bring something into existence and cause or enable it to continue.	
credential	Information passed from one entity to another that is used to establish the sending entity's access rights.	
critical function	Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.	
critical infrastructure	System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	
critical service	A service that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.	
criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (NIST SP 800-60).	
cyber incident ✓ <5 ADs referenced the term	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.	
cyber supply chain risk assessment process	The foundational task in the cyber supply chain risk assessment process, cyber supply chain risk assessments are aimed at identifying and assessing applicable risk of Information and operational technology (IT/OT) outsourcing, diverse distribution routes, assorted technologies, laws, policies, procedures, and practices.	
Cyber Supply Chain Risk Management Plan	A plan that includes confidentiality, integrity, and availability controls for mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.	
cyber supply chain risk management process	A detailed description of the steps necessary to mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.	

TERM	DEFINITION	DEFINED WITHIN
cyber threat intelligence	Organized, analyzed and refined information about potential or current attacks that threaten an organization. The primary purpose of threat intelligence is helping organizations understand the risks of the most common and severe external threats, such as zero-day threats, advanced persistent threats (APTs) and exploits. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types that are most likely to affect a particular organization's environment. Threat intelligence includes in-depth information about specific threats to help an organization protect itself from the types of attacks that could do them the most damage. In a military, business or security context, intelligence is information that provides an organization with decision support and possibly a strategic advantage. Threat intelligence is a component of security intelligence and, like SI, includes both the information relevant to protecting an organization from external and inside threats as well as the processes, policies and tools designed to gather and analyze that information. Threat intelligence services provide organizations with current information related to potential attack sources relevant to their businesses; some also offer consultation service.	
cybersecurity	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: - Availability - Integrity, which may include authenticity and non-repudiation - Confidentiality	
cybersecurity activity	Security controls that are specific to the realm of Cybersecurity.	✓
Cybersecurity Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Cybersecurity Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes.".	✓
cybersecurity event	Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.	
Cybersecurity Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.	✓
Cybersecurity Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.	✓
cybersecurity function ***cyber security function*✓** <5 ADs referenced the term	One of the main components of the Cybersecurity Framework. Cybersecurity functions provide the highest level of structure for organizing basic cybersecurity activities into Cybersecurity Categories and Cybersecurity Subcategories. The five Cybersecurity functions are the Identify function, Protect function, Detect function, Respond function, and Recover function.	✓

TERM	DEFINITION	DEFINED WITHIN
cybersecurity law, rule, or regulation	Any federal, state, or local statute or ordinance or any rule or regulation adopted according to any federal, state, or local statute or ordinance that deals specifically with the topic of protecting or defending computerized environments, organizational computerized assets, and user's computerized assets.	
Cybersecurity outcome	A Cybersecurity outcome is the business need defined and tiered implementation of the outcomes listed in either the Categories or Subcategories section of Table 2 in the NIST Cybersecurity Framework.	✓
Cybersecurity Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.	✓
cybersecurity risk	A risk to organizational operations, (including mission, functions, image, and reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information, Information Technology, and/or Operations Technology.	
cybersecurity risk management	The process of identifying risks and vulnerabilities and applying administrative actions and comprehensive solutions to ensure that the organization is adequately protected.	
cybersecurity roles and responsibilities	The functions and duties of personnel who are responsible for preventing cybersecurity events that disrupt operations or affected parties, assigned and performed in conformance with pertinent laws and standards.	
Cybersecurity Subcategory	The subdivision of a Cybersecurity Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated.".	✓
cybersecurity training	Activities that are used to teach people about tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.	
data	A subset of information in an electronic format that allows it to be retrieved or transmitted. (CNSSI-4009)	
data flow	The path of data from input to output, which includes the traveling of data through the communication lines, routers, switches and firewalls as well as processing through various applications on servers that process the data from user input to storage in the organizations central database.	
data leakage	An unauthorized data transfer out of a computer or data center.	
Data-At-Rest	Refers to all data stored on hard drives, thumb drives, DVDs, CDs, floppy diskettes, and similar storage media. It excludes data that is traversing a network or temporarily residing in computer memory to be read or updated.	
data-in-motion	Data being transferred between devices, such as data being sent from one application to another.	

TERM	DEFINITION	DEFINED WITHIN
define	To state or describe exactly the nature, scope, or meaning of something.	
delivery	The supply or provision of something.	
dependency	A relationship between processes or activities that directly or indirectly relies upon another process or activity to occur, begin, or finish.	
destroy	To render target data recovery infeasible and media unusable for the storage of data.	
detect	Discover, investigate, or discern the existence or presence of something.	
Detect Function	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.	✓
detective activity	An activity designed to identify undesirable events that do occur and alert management about what has happened. This enables management to take corrective action promptly.	
determine	To establish or ascertain exactly as a result of research or calculation.	
develop and implement	To design, create, and put something into effect.	
development environment	The set of processes and programming tools used to develop, test, and debug an application or program.	
device	A generic term for a server, storage, client platform, computer, or any part of a computer other than the CPU or working memory.	
dispose of	Get rid of by throwing away or giving or selling to someone else.	
document	To record something in detail through photography, writing, or other form.	
during	This limits a Control or Mandate's secondary verb to be put into play as the event is happening.	
effectiveness	The degree to which information is relevant and pertinent to the business process as well as delivered in a timely, correct, consistent, and usable manner.	
establish	To start something that will last for a long time, or to create or set something in a particular way.	
establish and implement	To lay the groundwork for something and then put it into practice.	
establish and maintain	To lay the groundwork for something and uphold it or ensure continuation by requiring maintenance.	

TERM	DEFINITION	DEFINED WITHIN
event	Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. (CNSSI-4009).	
event data	Any data that you want to measure about an event.	
event information	The data fields and information that needs to be captured during monitoring so that the organization knows what happened when the event was triggered.	
execute	To carry out fully or put something completely into effect.	
external information system	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.	
external service provider	An independent business that provides its services to other business.	
facility	A place, amenity, or piece of equipment provided for a particular purpose.	
forensics	As it relates to information security, the application of investigative tools and analysis techniques to gather evidence from computer resources to determine the cause of data compromises.	
Governance, Risk, and Compliance framework	The overall structure of procedures of how an organization is controlled and directed , how an organization identifies and mitigates risk, and how the organization adheres to pertinent rules, standards, and regulations that defines the scope, objectives, and activities regrading such procedures.	
hardware integrity	The assurance that any given hardware asset is not a counterfeit, or otherwise falsely represented as being whole and intact as measured against original specifications.	
human resources process	The steps necessary to support the general management of the organizational workforce, including staffing, employee compensation and benefits, and defining/designing work.	
identify	To establish, indicate, or verify who or what someone or something is.	
identify and document	Establish, indicate, or verify who or what someone or something is and record that in detail through photography, writing, or other form.	
Identify Function	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.	✓
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.	

TERM	DEFINITION	DEFINED WITHIN
impact	A measure of the effect of an incident, problem, or change on business processes; often based on how service levels will be affected; used with urgency to assign priority.	
implement	To put a plan, policy, decision, agreement, etc. into action or effect.	
improve	To make or become better; enhance in value or quantity.	
incident	An event that disrupts the service or operations of an organization.	
incident alert	Any form of security alert, security alarm, or logged event notification that has been triggered by any form of detection. The triggering of an incident alert begins the incident response process.	
incident alert threshold	The magnitude or intensity that must be exceeded before a detected incident triggers an alert, who receives the alert, and the priority of the alert.	
incident containment process	An established or official method for implementing the policy for incident containment or performing the tasks, processes, or operations to limit and prevent further damage from happening after an incident occurs, along with ensuring that there is no destruction of forensic evidence that may be needed for future legal actions which must be executed in the same manner in order to obtain the same results in the same circumstances.	
incident management process	An activity undertaken to direct personnel and resources to respond to an incident.	
incident monitoring process	An established or official method for implementing the policy for incident monitoring or performing the tasks, processes, or operations to monitor for incidents which must be executed in the same manner in order to obtain the same results in the same circumstances.	
incident monitoring program	The documented activities, policies, and procedures within an organization for organizing and directing all activities undertaken to review, track, evaluate, and report on the status of incidents.	
incident monitoring roles and responsibilities	The position and collection of tasks, duties, obligations that participants undertake to perform the daily and all special tasks associated with reviewing, trackIng, evaluatIng, and reportIng on the status of incidents..	
incident response process	An established or official method for implementing the policy for incident response or performing the tasks, processes, or operations to address and manage the aftermath of a disaster or other significant event that may affect the organization’s people or ability to function productively which must be executed in the same manner in order to obtain the same results in the same circumstances.	
incident response program	A documented approach for organizing and directing all activities undertaken to handle known security breaches or attacks in such a way as to limit damage and reduce the time it takes for the organization to recover time and costs.	

TERM	DEFINITION	DEFINED WITHIN
incident response roles and responsibilities	The position and collection of tasks, duties, obligations that participants undertake to perform the daily and all special tasks associated with managing the aftermath of a disaster or other significant event that may affect the organization's people or ability to function productively..	
include	Make part of a whole or set.	
incorporate	To include, take in or contain something as part of a whole.	
individual	A human being.	
industry sector	The world of business and commerce is often divided up in to a selection of broad and commonly recognised groups, called sectors. Often a more general term, a sector represents a group of industries and markets that share common attributes.	
inform	Give someone facts or information.	
information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.	
Information Security policy	The rules and guidelines of an organization on how to ensure the confidentiality, integrity, and availability of the organization's information.	
information security procedure	The documented series of steps on how to establish and maintain the confidentiality, integrity, and availability of information.	
information security process	The activities associated with establishing and maintaining the confidentiality, integrity, and availability of data and information.	
information security roles and responsibilities	The position and collection of tasks, duties, obligations that participants undertake to perform the daily and all special tasks in the role of information security.	
information sharing forum	An assembly in which participants share problems, solutions, updates, and data on topics relevant to its discourse.	
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.	
information system component	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.	
information technology supplier	Information systems, components and services providers used for an organization’s internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization’s buyers.	

TERM	DEFINITION	DEFINED WITHIN
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Cybersecurity Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the “Data-in-transit is protected” Subcategory of the “Data Security” Category in the “Protect” function.	✓
integrity check mechanism	Any software, hardware, or methodology that checks a program, system, or records for unauthorized modifications.	
interaction	A mutual or reciprocal action; interacting.	
interested personnel	This role focuses on persons or organizations that have a recognizable stake in the outcome of a court matter or who are potentially being affected by a situation or hoping to make money off of the situation. Any individual or organization that has a recognizable stake in the outcome of a court matter, may be affected by a situation, or make money from the situation should be assigned to this role.	
inventory	To make a comprehensive complete list of things.	
investigate	To carry out a formal or systematic inquiry to discover and examine the facts of an event, incident, etc. in order to establish the truth.	
know	To have an understanding of or information concerning something.	
law enforcement authority	The various government agencies responsible for preventing crime, apprehending criminals, and enforcing laws.	
least functionality principle	In information security, computer science, and configuration management the limiting of access to only that information and resources that are necessary for its legitimate purpose.	
least privilege	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	
lessons learned	A set of statements captured after completion of a project or a portion of a project that describes in a neutral way what did or did not work, along with a statement regarding the risk of ignoring the lesson.	
likelihood	The state or fact of something's being likely; probability.	
limit	To restrict or assign boundaries to something.	
log	To record an event or transaction in an organized record-keeping system, usually sequenced in the order they occurred.	
maintain	To keep up; continue a condition or situation; carry on.	
maintenance	The process of making repairs and keeping components of an asset in good condition so that the asset may remain in operating condition and last its entire useful life.	

TERM	DEFINITION	DEFINED WITHIN
malicious code	Software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner’s data, applications, or operating system. Such software typically enters a network during many business-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.	
manage	To handle or control the behavior, movement, or function of a person, animal, or thing.	
map	To diagram data that is to be exchanged electronically, including how it is to be used and what business management systems need it; a preliminary step for developing an applications link.	
meet	Fulfill or satisfy (a need, requirement, or condition).	
mission	A statement of what an organization will achieve.	
mitigate	To lessen or to try to lessen the severity, pain, seriousness, extent, or gravity of.	
mobile code ✓ <5 ADs referenced the term	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.	✓
monitor	To watch and check the progress or quality of something over a period of time; keep under regular surveillance.	
multiple sources	Information classified based on two or more source documents, classification guides or combination of both.	
network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.	
network activity baseline	Establishing a trusted baseline document involves identifying the following: - network data points of interest - length of the baseline data collection period - methods and tools used to collect and store data Suggested network data points of interest include the following: - a list of predetermined devices a given workstation or server should communicate with - VPN usage, including access times, bandwidth and resources used, source IP addresses, and geolocation information - the known set of ports and protocols in use by the network - firewall and intrusion detection system logs - normal traffic patterns and flows.	
network integrity	The state of a computer network where it is performing its intended functions without being degraded or impaired by changes or disruptions in its internal or external environments. A network is functioning properly when several things occur: applications and client get enough network availability, applications and clients get proper bandwidth, network security does its job during both peacetime and attack, and network management has complete control of the entire network.	
network segregation	Developing and enforcing a ruleset controlling which computing devices are permitted to communicate with which other computing devices.	

TERM	DEFINITION	DEFINED WITHIN
objective	A projected state of affairs that a person or a system plans or intends to achieve a personal or organizational desired end-point in some sort of assumed development. Many people endeavor to reach goals within a finite time by setting deadlines.	
operating state	Distinct operating modes (which typically include specific Information Technology and Operations Technology configurations as well as alternate or modified procedures) that have been designed and implemented for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resiliency, reliability, and/or cybersecurity. For example, a shift from the normal state of operation to a high-security operating mode may be invoked in response to a declared cybersecurity incident of sufficient severity. The high-security operating state may trade off efficiency and ease of use in favor of increased security by blocking remote access and requiring a higher level of authentication and authorization for certain commands until a return to the normal state of operation is deemed safe.	
operation	An organized activity involving multiple people.	
organization	This group focuses on corporate bodies, businesses, federal agencies and their operational elements, and any entity that has people, resources, and budgets. Any of these bodies should be assigned to this group.	
organizational objective	Performance targets set by an organization.	
organizational risk tolerance	The level of risk an organization is willing to take in order to achieve a potential desired result.	
partner	An associate in an activity or endeavor or sphere of common interest.	
perform	To carry out an action, task, or function.	
personnel	People who are employed by and work directly within an organization.	
personnel activity	Any duty or action performed by a staff member.	
physical access	The ability of people to physically gain access to a computer system or facility.	
physical access control	A mechanism, system, or barrier that prevents unauthorized physical access to an area or a facility.	
physical environment	The physical external surrounding and conditions in which something exists.	
physical operating environment authority document	Statutes, regulations, safe harbors, audit guidelines, best practices, Service Level Agreements, Contractual Obligations, organizational policies and procedures, and any other documents that defines the temperatures, humidity levels, electromagnetic levels, vibration levels, power levels, and space required for any device to operate properly.	
place	A physical environment, point, or position; portion of space; location.	

TERM	DEFINITION	DEFINED WITHIN
policy	An official expression of principles that direct an organization's operations.	
policy and procedure	A set of policies are principles, rules, and guidelines formulated or adopted by an organization to reach its long-term goals and typically published in a booklet or other form that is widely accessible. Policies and procedures are designed to influence and determine all major decisions and actions, and all activities take place within the boundaries set by them. Procedures are the specific methods employed to express policies in action in day-to-day operations of the organization. Together, policies and procedures ensure that a point of view held by the governing body of an organization is translated into steps that result in an outcome compatible with that view.	
potential impact	The loss of confidentiality, integrity, or availability could be expected to have: • a limited adverse effect (FIPS 199 low); • a serious adverse effect (FIPS 199 moderate); or • a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.	
prioritize	To determine the order for dealing with a series of items or tasks according to their relative importance.	
priority	A category based on impact and urgency used to identify the relative importance of an incident, problem, or change and the required time for action to be taken. For example, the SLA may state that priority 2 incidents must be resolved within 12 hours.	
privileged user	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.	
procedure	An established or official method for implementing a policy or performing a task or operation which must be executed in the same manner in order to obtain the same results in the same circumstances.	
process	A series of operations performed by a computer.	
production environment	Production environment is a term used mostly by developers to describe the setting where software and other products are actually put into operation for their intended uses by end users. A production environment can be thought of as a real-time setting where programs are run and hardware setups are installed and relied on for organization or commercial daily operations.	
proof	To proofread.	
protect	To shield or defend from danger, harm, injury, loss, destruction, or damage.	
Protect Function	A Cybersecurity Function that focuses on developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services.	✓
protection	The activity of keeping someone or something safe from harm or injury.	

TERM	DEFINITION	DEFINED WITHIN
protective measure	Any precautionary action, procedure or installation conceived or undertaken to guard or defend from harm persons, property or the environment.	
protective technology	Special tamper-evident features and materials employed for the purpose of detecting tampering and deterring attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and keying material.	
provide	To supply or make something available for use.	
Public Relations	The professional maintenance of a favorable public image by a company or other organization or a famous person.	
receive	To be given, presented with, paid, or come into possession of something.	
record	Anything that is put down in permanent form and preserved as evidence.	
Recover Function	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.	✓
recovery action	An action that is undertaken to return something to a normal state.	
recovery plan	The written expression of a recovery process which consists of defining rules, processes, and disciplines to ensure that the critical business processes will continue to function if there is a failure of one or more of the information processing or telecommunications resources upon which their operations depends. The following are key elements to a disaster recovery plan: 1) Establish a planning group, 2) Perform risk assessment and audits, 3) Establish priorities for applications and networks, 4) Develop recovery strategies, 5) Prepare inventory and documentation of the plan, 6) Develop verification criteria and procedures, 5) Implement the plan.	
recovery planning	The activities undertaken to define a recovery process which consists of defining rules, processes, and disciplines to ensure that the critical business processes will continue to function if there is a failure of one or more of the information processing or telecommunications resources upon which their operations depends.	
recovery process	The steps taken to restore a service, configurable item, etc. to a working state.	
recovery strategy	A strategy to resume the minimum set of critical services identified in the business impact analysis (e.g. use of another delivery channel to provide the same service.	
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).	
remote maintenance	Offsite monitor, service, repair, and diagnostic activities on assets performed by secure communication through an external network.	
removable storage media	Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no	

TERM	DEFINITION	DEFINED WITHIN
	independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), thumb drives, pen drives, and similar USB storage devices.	
repair	Restore something damaged, faulty, or worn to a good condition.	
report	To give a spoken or written account of something that has been seen, done etc.	
reputation	The beliefs, opinion, or social evaluation of the public about someone or something.	
resource	An asset available for use.	
Respond Function	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	✓
response activity	Any task performed by an organization in reaction to discovered risks.	
response and recovery strategy	A systematic plan of action consisting of documented procedures for mitigating and recovering from a disruptive event.	
response plan	A document detailing the steps that must be taken, or the activities that must be performed well, in response to risk assessment or audit findings.	
restoration operation	An organized activity to restore something.	
restrict	To confine or put a limit on; keep under control; restrain.	
review	To examine or evaluate formally with the intent of making changes if necessary.	
risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: • the adverse impacts that would arise if the circumstance or event occurs; and • the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.	
risk analysis	The purpose of this task is to examine and identify the risks to the system, determine the probability of occurrence, analyze the related vulnerabilities of the system, the resulting impact, and the additional safeguards that mitigate this impact.	
risk decision	A decision by the leadership of an organization to accept an option having a given risk function in preference to another, or in preference to taking no action.	
risk management process	The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating,monitoring and reviewing risk	
risk management strategy	A plan of action for analyzing and prioritizing risks to organizational operations, assets, and personal in alignment with the organization's mission and business objectives.	

TERM	DEFINITION	DEFINED WITHIN
risk response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, resources, and other organizations.	
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.	
role	A set of responsibilities defined in a process and assigned to a person or team.	
roles and responsibilities	The position and collection of tasks, duties, obligations that participants undertake to complete a project.	
security control	A safeguard or countermeasure to avoid, counteract or minimize security risks relating to personal property, or any company property. For business-to-business facing organizations whose service may affect the financial statements of the other company, the prospect may require successful audit reports of policy controls.	
security personnel	Individuals who protect people, facilities, and information for an organization.	
security policy	The statement of required protection of the information objects that documents an organization's philosophy of managing, protecting, and distributing its computing and information assets. The set of security rules enforced by the system's security features.	
security process	A series of actions that ensure the protection of data.	
senior executive	A long standing and top ranking member of the management of an organization.	
separate	To move or be apart; detach; disconnect.	
separation of duty	Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.	
share	To have something in common or use jointly.	
software platform	A major piece of software, as an operating system, an operating environment, or a database, under which various smaller application programs can be designed to run.	
source	The place, person, or thing where something begins or comes into being.	
stakeholder	An individual who has an interest in something, e.g., a corporation, and is affected by decisions and activities regarding that issue.	
supplier	Product and service providers used for an organization’s internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization’s Buyers.	
supply chain	A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.	

TERM	DEFINITION	DEFINED WITHIN
supply chain risk	A risk measured by the likelihood and severity of damage if an Information Technology or Operations Technology system is compromised by a supply chain attack, and takes into account the importance of the system and the impact of compromise on organizational operations and assets, individuals, other organizations, and the Nation. Supply chain attacks may involve manipulating computing system hardware, software, or services at any point during the life cycle. Supply chain attacks are typically conducted or facilitated by individuals or organizations that have access through commercial ties, leading to stolen critical data and technology, corruption of the system/ infrastructure, and/or disabling of mission-critical operations.	
supply chain risk management process	The implementation through controls and structures of strategies to manage both everyday and exceptional risks along the supply chain based on continuous risk assessment with the objective of reducing vulnerability and ensuring continuity.	
support	To provide aid or give assistance to.	
suspicious activity	Activities that give the idea or impression that they are of questionable, dishonest, or of dangerous character or conditions.	
system	An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.	
System Development Life Cycle	A series of stages that the process of system development goes through in order to design and produce a system.	
taxonomy	A structure or scheme used for classifying materials or concepts into a hierarchy of categories and subcategories.	✓
technical security solution	Hardware, software, and methodologies for protecting computerized assets from, or resilience against, potential harm from external forces.	
test	To ascertain the performance, reliability, or quality of something.	
test environment	A controlled environment in which tests will be run on configuration items, builds, processes, IT services, etc.	
test result	A formal document defining the subject of the test, the test plan, approach, analysis tools, and conclusions found during the testing process.	
third party	A person or group besides the two primarily involved in a situation, agreement, business, etc.	
third party contract	Means a contract or purchase order awarded by the Recipient or subrecipient to a vendor or contractor.	
threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential	

TERM	DEFINITION	DEFINED WITHIN
	for a threat-source to successfully exploit a particular information system vulnerability.	
Threat and Vulnerability Management process	A process that includes vulnerability assessments, vulnerability scanning, penetration testing. Also included in the process is the cataloging of the assets that are in scope, assigning value and importance to those resources, and mitigating or eliminating any vulnerabilities discovered during the process.	
timely manner	As quickly as is reasonable in a particular situation.	
train	To teach a person or animal a particular skill or type of behavior through sustained practice and instruction.	
transfer	To change possession of property, a right, or a responsibility to another.	
unapproved Information Technology resource	An unsanctioned Information Technology resource.	
unauthorized access	Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.	
unauthorized mobile code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics -- that has not been permitted by the controlling authority.	
unauthorized personnel	Employees who do not have the right or permission to access data (or a facility containing data).	
understand	To perceive the intended meaning, significance, explanation, or cause of something.	
update	To modernize or bring up to date.	
use	The action of employing something or the state of being put into action for some purpose.	
user	This role focuses on the use or operation of a system, having an account on a system, accessing a cryptographic module to obtain cryptographic services, or receiving or using services from an automated information system facility. Any individual or organization that uses or operates a system, has an account on a system, accesses cryptographic modules to obtain cryptographic services, or uses or receives services from an automated information system facility should be assigned to this role.	
verify	To make certain or prove that something is true or accurate; confirm; substantiate.	
vulnerability	A weakness in an information system, administrative controls, internal controls, system security practices and procedures, implementation, or physical layout that could be accidentally triggered or intentionally exploited by a threat in order to gain unauthorized access to information or disrupt processing.	

TERM	DEFINITION	DEFINED WITHIN
Vulnerability Management plan	This purpose of this plan is to establish the organization's assessment and testing process to ensure systems are less susceptible to cyber attack.	
vulnerability scan	The check of a system for known vulnerabilities from beginning to end with resultant errors, and status information.	
workforce	The individuals engaged in or available for work in a country, industry or organization.	

For more information on the UCF Mapper™, click HERE.