NJCCIC Cybersecurity Program Controls Assessment Guidelines

Published by:
NJ Cybersecurity and Communications Integration Cell
September 2018

Table of Contents

INTRODUCTION

The NJCCIC is a component organization within the New Jersey Office of Homeland Security and Preparedness' Division of Cybersecurity. The NJCCIC is comprised of cybersecurity subject matter experts from the Division of Cybersecurity, the New Jersey State Police (NJSP), and the New Jersey Office of Information Technology (OIT). Collectively, they act as the State's one-stop shop for coordinating cybersecurity information sharing and incident reporting, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors.

As New Jersey's citizens, businesses, schools, and governments continue to expand their online footprint, they are more exposed to cyber-attacks. The NJCCIC collects and evaluates cyber threat intelligence from federal, state, and local sources and disseminates products including threat profiles on Ransomware, Exploit Kits, Point-of-Sale Malware, Trojans, and other cyber threats. A primary focus of the NJCCIC's efforts is to develop partnerships with key critical infrastructure sectors across New Jersey, the business community, academia, and local governments in order to share threat information in near real-time and to assist them in managing cyber risks.

The NJCCIC also provides strategies and tactics that businesses, as well as local governments, academic institutions, and other organizations can use to help manage cyber risk. Towards that end the NJCCIC has developed the NJCCIC Cybersecurity Program Controls Assessment to help organizations address cyber risks by gauging their maturity across 33 controls areas that the NJCCIC identifies as essential to an effective and comprehensive cybersecurity program. While organizations may structure their cybersecurity programs differently, the NJCCIC considers the following 33 Control Areas as essential to an effective program.

SCOPE AND APPLICABILITY

The NJCCIC Cybersecurity Program Controls Assessment has been created to ensure alignment with industry best practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations; the Center for Internet Security (CIS) Top 20 Critical Security Controls; and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

The Cybersecurity Program Controls Assessment is intended to be a general controls assessment applicable to all industries and sectors. It is intended to be advisory in nature only. Organizations that have specific cybersecurity requirements as defined by law, regulation, contract, or policy should not conclude that this assessment is a substitute for adherence to those requirements.

Unless otherwise required by applicable law, regulation, contract, or policy the completion and submission of this assessment is completely voluntary. Submitting organizations will be enrolled as an NJCCIC member and receive the NJCCIC's weekly bulletin, threat alerts and advisories, opportunities for cybersecurity training programs, and other cybersecurity services and resources specific to the submitting organization's needs.

CONTROL AREAS

The following 33 information security control areas are intended to provide guidance and act as a frame of reference for organizations in the comprehensiveness and sufficiency of their cybersecurity programs. While organizations may structure their cybersecurity programs differently, the NJCCIC considers the following 33 Control Areas as essential to an effective information security program.

INFORMATION SECURITY PROGRAM MANAGEMENT (PM)

The organization establishes and maintains a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk. Information security program management includes, but is not limited to, the following:

- Establishment of a management structure and responsibility for information security;
- Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed below;
- Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and
- Independent review of the effectiveness of the organization's information security program.

COMPLIANCE (CP)

The organization develops, implements, and governs processes to ensure its compliance with all applicable statutory, regulatory, contractual, and internal policy obligations. Ensuring compliance includes but is not limited:

- Statutory, Regulatory, and Contractual Compliance
- Security controls oversight
- Periodically conducting security assessments

PERSONNEL SECURITY (PS)

The organization implements processes to ensure all personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner. Workforce security controls include, but are not limited to:

- Position descriptions that include appropriate language regarding each role's security requirements;
- To the extent permitted by law, employment screening checks are conducted and successfully passed for all personnel prior to beginning work or being granted access to organization information assets;
- Rules of behavior are established and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to the organization's information and information systems;
- Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate;
- Disabling system access for terminated personnel and collecting all organization owned assets prior to the individual's departure; and
- Procedures are implemented that ensure all personnel are aware of their duty to protect organizational information assets and their responsibility to immediately report any suspected information security incidents.

SECURITY AWARENESS AND TRAINING (AW)

The organization provides information security awareness and training to ensure employees are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory, regulatory, contractual, and policy requirements that are intended to protect information systems and information from a loss of confidentiality, integrity, availability and privacy. Security awareness and training includes, but is not limited to:

- Employees are provided with security awareness training upon hire and at least annually, thereafter;
- Security awareness training records are maintained as part of the employee's personnel record;
- Role-based security training is provided to individuals with respect to their duties or responsibilities (e.g. network and systems administrators require specific security training in accordance with their job functions); and
- Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.

RISK MANAGEMENT (RM)

The organization establishes requirements for the identification, assessment, and treatment of information security risks to organization operations, information, and/or information systems. Risk management includes, but is not limited to:

- Categorizing systems and information based on their criticality and sensitivity;
- Ensuring risks are identified, documented and assigned to appropriate personnel for assessment and treatment;
- Ensuring risk assessments are conducted throughout the lifecycles of information systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met; and
- Mitigating risks to an acceptable level and prioritizing remediation actions based on risk criteria and establishing timelines for remediation. Risk treatment may also include the acceptance or transfer of risk.

PRIVACY (PR)

The organization establishes appropriate processes and safeguards necessary to protect the personally identifiable information (PII) that the organization collects, stores, processes, uses, and transmits. Privacy controls and processes include, but are not limited to:

- Ensuring only the minimum amount of PII necessary to carry out the business function, and in accordance with applicable laws and regulations, is collected and stored;
- Safeguarding PII through the implementation of administrative, physical, and technical controls (e.g. access controls, encryption and tokenization, etc.); and
- Securely deleting PII when no longer necessary for business or legal purposes.

INFORMATION ASSET MANAGEMENT (AM)

The organization implements administrative, technical, and physical controls necessary to safeguard information technology assets from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate or accidental. Asset management controls include, but are not limited to:

- Information technology asset identification and inventory;
- Assigning custodianship of assets; and
- Restricting the use of non-authorized devices.

SECURITY CATEGORIZATION (SC)

The organization implements processes that classify information and categorize information systems throughout their lifecycles according to their sensitivity and criticality, along with the risks and impact should there be a loss of confidentiality, integrity, availability, or privacy. Information classification and system categorization includes labeling and handling requirements. Security Categorization controls include, but are not limited to, the following:

- Implementing a data protection policy;
- Classifying data and information systems in accordance with their sensitivity and criticality;
- Masking sensitive data that is displayed or printed; and
- Implementing handling and labeling procedures.

MEDIA PROTECTION (MP)

The organization establishes controls to ensure data and information, in all forms and mediums, are protected throughout their lifecycles based on their sensitivity, value, and criticality, and the impact that a loss of confidentiality, integrity, availability, and privacy would have on the organization, business partners, or individuals. Media protections include, but are not limited to:

- Media storage/access/transportation;
- Maintenance of sensitive data inventories;
- Application of cryptographic protections;
- Restricting the use of portable storage devices;
- Establishing records retention requirements in accordance with business objectives and statutory and regulatory obligations; and
- Media disposal/sanitization.

CRYPTOGRAPHIC PROTECTION (CR)

The organization employs cryptographic safeguards to protect sensitive information in transmission, in use, and at rest, from a loss of confidentiality, unauthorized access, or disclosure. Cryptographic protections include, but are not limited to:

- Using industry standard encryption algorithms;
- Establishing requirements for encryption of data in transit;
- Establishing requirements for encryption of data at rest; and
- Implementing cryptographic key management processes and controls.

ACCESS MANAGEMENT (AC)

The organization establishes security requirements and ensures appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the organization's information systems. Access management includes, but is not limited to:

- Ensuring the principle of least privilege is applied for specific duties and information systems (including specific functions, ports, protocols, and services), so processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions;
- Implementing account management processes for registration, updates, changes and de-provisioning of system access;
- Applying the principles of least privilege when provisioning access to organizational assets;
- Provisioning access according to an individual's role and business requirements for such access;
- Implementing the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people; and
- Conducting periodic reviews of access authorizations and controls.

IDENTITY AND AUTHENTICATION (IA)

The organization establishes procedures and implements identification, authorization, and authentication controls to ensure only authorized individuals, systems, and processes can access the organization's information and information systems. Identity and authentication provides a level of assurance that individuals who log into a system are who they say they are. Identity and authentication controls include, but are not limited to:

- Establishing and managing unique identifiers (e.g. User-IDs) and secure authenticators (e.g. passwords, biometrics, personal identification numbers, etc.) to support nonrepudiation of activities by users or processes; and
- Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the organization's systems.

REMOTE ACCESS (RA)

The organization strictly controls remote access to the organization's internal networks, systems, applications, and services. Appropriate authorizations and technical security controls are implemented prior to remote access being established. Remote access controls include, but are not limited to:

- Establishing centralized management of the organization's remote access infrastructure;

- Implementing technical security controls (e.g. encryption, multi-factor authentication, IP whitelisting, geo-fencing); and
- Training users in regard to information security risks and best practices related to remote access use.

SECURITY ENGINEERING AND ARCHITECTURE (SE)

The organization employs security engineering and architecture principles for all information technology assets, such that they incorporate industry recognized leading security practices and address applicable statutory and regulatory obligations. Applying security engineering and architecture principles includes, but is not limited to, the following:

- Implementing configuration standards that are consistent with industry-accepted system hardening standards and addressing known security vulnerabilities for all system components;
- Establishing a defense in-depth security posture that includes layered technical, administrative, and physical controls;
- Incorporating security requirements into the systems throughout their life cycles;
- Delineating physical and logical security boundaries;
- Tailoring security controls to meet organizational and operational needs;
- Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;
- Implementing controls and procedures to ensure critical systems fail-secure and fail-safe in known states; and
- Ensuring information system clock synchronization across the organization.

CONFIGURATION MANAGEMENT (CM)

The organization ensures that baseline configuration settings are established and maintained in order to protect the confidentiality, integrity, and availability of all information technology assets. Secure configuration management includes, but is not limited to:

- Hardening systems through baseline configurations; and
- Configuring systems in accordance with the principle of least privilege to ensure processes operate at privilege levels no higher than necessary to accomplish required functions.

ENDPOINT SECURITY (ES)

The organization ensures that endpoint devices are properly configured, and measures are implemented to protect the organization's information and information systems from a loss of confidentiality, integrity, and availability. Endpoint security includes, but is not limited to:

- Maintaining an accurate and updated inventory of endpoint devices;
- Applying security categorizations and implementing commensurate safeguards on endpoints;
- Maintaining currency with operating system and software updates and patches;
- Establishing physical and logical access controls;
- Applying data protection measures (e.g. cryptographic protections);
- Implementing anti-malware software, host-based firewalls, and port and device controls;
- Implementing host intrusion detection and prevention systems (HIDS/HIPS) where applicable;
- Restricting access and/or use of ports and I/O devices; and
- Ensuring audit logging is implemented and logs are reviewed on a continuous basis.

ICS/SCADA/OT SECURITY (OT)

The organization implements controls and processes to ensure risks, including risks to human safety, are accounted for and managed in the use of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems and Operational Technologies (OT). ICS/SCADA/OT Security requires the application of all of the enumerated control areas included here in this document, including, but not limited to:

- Conducting risk assessments prior to implementation and throughout the lifecycles of ICS/SCADA/OT assets;
- Developing policies and standards specific to ICS/SCADA/OT assets;
- Ensuring the secure configuration of ICS/SCADA/OT assets;
- Segmenting ICS/SCADA/OT networks from the rest of the organization's networks;
- Ensuring least privilege and strong authentication controls are implemented;
- Implementing redundant designs or failover capabilities to prevent business disruption or physical damage; and
- Conducting regular maintenance on ICS/SCADA/OT systems.

INTERNET OF THINGS SECURITY (IT)

The organization implements controls and processes to ensure risks are accounted for and managed in the use of Internet of Things (IoT) devices including, but not limited to, physical devices, vehicles, appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these devices to connect and exchange data. IoT security includes, but is not limited to, the following:

- Developing policies and standards specific to IoT assets;
- Ensuring the secure configuration of IoT assets;
- Conducting risk assessments prior to implementation, and throughout the lifecycles of IoT assets;
- Segmenting IoT networks from the rest of the organization's networks; and
- Ensuring least privilege and strong authentication controls are implemented.

MOBILE DEVICE SECURITY (MD)

The organization establishes administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for organizational business purposes. Mobile device security includes, but is not limited to, the following:

- Establishing requirements for authorization to use mobile devices for organizational business purposes;
- Establishing Bring Your Own Device (BYOD) processes and restrictions;
- Establishing physical and logical access controls;
- Implementing network access restrictions for mobile devices;
- Implementing mobile device management solutions to provide centralized management of mobile devices and to ensure technical security controls (e.g. encryption, authentication, remote-wipe, etc.) are implemented and updated as necessary;
- Establishing approved application stores from which applications can be acquired;
- Establishing lists of approved applications that can be used; and
- Training of mobile device users regarding security and safety.

NETWORK SECURITY (NS)

The organization implements defense-in-depth and least privilege strategies for securing the information technology networks that they operate. To ensure information technology resources are available to authorized network clients and protected from unauthorized access, organizations must:

- Include protection mechanisms for network communications and infrastructure (e.g. layered defenses, denial of service protection, encryption for data in transit, etc.);
- Include protection mechanisms for network boundaries (e.g. limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.);
- Control the flow of information (e.g. deny traffic by default/allow by exception, implement Access Control Lists, etc.); and
- Control access to the organization's information systems (e.g. network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).

CLOUD SECURITY (CL)

The organization establishes security requirements that govern the use of private, public, and hybrid cloud environments to ensure risks associated with a potential loss of confidentiality, integrity, availability, and privacy are managed. This includes, but is not limited to, ensuring the following:

- Security is accounted for in the acquisition and development of cloud services;
- The design, configuration, and implementation of cloud-based applications, infrastructure and system-system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations;
- Security roles and responsibilities for the organization and the cloud provider are delineated and documented; and
- Controls necessary to protect sensitive data in public cloud environments are implemented.

CHANGE MANAGEMENT (CH)

The organization establishes controls required to ensure change is managed effectively. Organizations must ensure changes are appropriately tested, validated, and documented before implementing any change on a production network. Change management provides the organization with the ability to handle changes in a controlled, predictable, and repeatable manner, and to identify, assess, and minimize the risks to operations and security. Change management controls include, but are not limited to, the following:

- Notifying all stakeholders of changes;
- Conducting a security impact analysis for changes; and
- Verifying security functionality after the changes have been made.

MAINTENANCE (MA)

Organizations implement processes and controls to ensure that information assets are properly maintained, thereby minimizing the risks from emerging information security threats and/or the potential loss of confidentiality, integrity, or availability due to system failures. Maintenance security includes, but is not limited to, the following:

- Conducting scheduled and timely maintenance;
- Ensuring individuals conducting maintenance operations are qualified and trustworthy; and
- Vetting, escorting, and monitoring third-parties conducting maintenance operations on the organization's information technology assets.

THREAT MANAGEMENT (TM)

The organization establishes a formalized mechanism to collect and disseminate actionable threat intelligence, thereby providing component units and individuals with the information necessary to effectively manage risk associated with new and emerging threats to the organization's information technology assets and operations. Threat intelligence includes, but is not limited to, the alerts, bulletins, advisories and best practice disseminated to water sector organizations by the NJCCIC. Other sources include US-CERT and the organization's technology vendors, among others.

VULNERABILITY AND PATCH MANAGEMENT (VU)

The organization implements proactive vulnerability identification, remediation, and patch management practices to minimize the risk of a loss of confidentiality, integrity, and availability of information system, networks, components, and applications. Vulnerability and patch management practices include but are not limited to the following:

- Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of the organization's systems and information, and the risks associated with a loss of confidentiality, integrity, availability, and/or privacy;
- Maintaining software and operating systems at the latest vendor-supported patch levels;
- Conducting penetration testing and red team exercises; and
- Employing qualified third-parties to conduct Independent vulnerability scanning, penetration testing, and red-team exercises

CONTINUOUS MONITORING (CO)

The organization implements continuous monitoring practices to establish and maintain situational awareness regarding potential threats to the confidentiality, integrity, availability,

privacy and safety of the organization's information and information systems through timely collection and review of security-related event logs. Continuous monitoring practices include, but are not limited to, the following:

- Centralizing the collection and monitoring of event logs;
- Ensuring the content of audit records includes all relevant security event information;
- Protection of audit records from tampering; and
- Detecting, investigating, and responding to incidents discovered through monitoring.

SYSTEM DEVELOPMENT AND ACQUISITION (SD)

The organization establishes security requirements necessary to ensure that systems and application software programs developed by the organization or third-parties (e.g. vendors, contractors, etc.) perform as intended to maintain information confidentiality, integrity, and availability, and the privacy and safety of individuals. System development and acquisition security practices include, but are not limited to, the following:

- Secure coding;
- Separation of development, testing and operational environments;
- Information input restrictions;
- Input data validation;
- Error handling;
- Security testing throughout development;
- Restrictions for access to program source code; and
- Security training of software developers and system implementers.

PROJECT AND RESOURCE MANAGEMENT (PM)

The organization ensures that controls necessary to appropriately manage risks are accounted for and implemented throughout the System Development Life Cycle (SDLC). Project and resource management security practices include, but are not limited to:

- Defining and implementing security requirements;
- Allocating resources required to protect systems and information; and
- Ensuring security requirements are accounted for throughout the SDLC.

CAPACITY AND PERFORMANCE MANAGEMENT (CA)

The organization implements processes and controls necessary to protect against avoidable impacts to operations by proactively managing the capacity and performance of its critical technologies and supporting infrastructure. Capacity and performance management practices include, but are not limited to, the following:

- Ensuring the availability, quality, and adequate capacity of compute, storage, memory and network resources are planned, prepared, and measured to deliver the required system performance and future capacity requirements; and
- Implementing resource priority controls to prevent or limit Denial of Service (DoS) effectiveness.

THIRD PARTY MANAGEMENT (TP)

The organization implements processes and controls to ensure that risks associated with third-parties (e.g. vendors, contractors, business partners, etc.) providing information technology equipment, software, and/or services are minimized or avoided. Third party management processes and controls include, but are not limited to:

- Tailored acquisition strategies, contracting tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;
- Due diligence security reviews of suppliers and third parties with access to the organization's systems and sensitive information;
- Third party interconnection security; and
- Independent testing and security assessments of supplier technologies and supplier organizations.

PHYSICAL AND ENVIRONMENTAL SECURITY (PE)

The organization establishes physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. The organization ensures appropriate environmental controls in facilities containing information systems and assets, to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions. Physical and environmental controls include, but are not limited to, the following:

- Physical access controls (e.g. locks, security gates and guards, etc.);
- Visitor controls;
- Security monitoring and auditing of physical access;
- Emergency shutoff;
- Emergency power;
- Emergency lighting;

- Fire protection;
- Temperature and humidity controls;
- Water damage protection; and
- Delivery and removal of information assets controls.

CONTINGENCY PLANNING (CT)

The organization develops, implements, tests, and maintains contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the organization. Contingency planning includes, but is not limited to:

- Backup and recovery strategies;
- Continuity of operations plans;
- Disaster recovery plans; and
- Crisis management plans.

INCIDENT RESPONSE (IR)

The organization maintains an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities include the following:

- Information security incident reporting awareness;
- Incident response planning and handling;
- Establishment of an incident response team;
- Contracts with external incident response services specialists; and
- Contacts with law enforcement cybersecurity units.

GLOSSARY: ACRONYMS AND KEY TERMS

ACRONYMS

ACL	Access Control List
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BPU	New Jersey Board of Public Utilities
BYOD	Bring Your Own Device
CDE	Cardholder Data Environment
CERT	Computer Emergency Response Team
COOP	Continuity of Operations Plan
DCS	Distributed Control System
DR	Disaster Recovery
I/O	Input/Output
ICS	Industrial Control System
IoT	Internet of Things
IR	Incident Response
ISIRT	Information Security Incident Response Team
HIPAA	Health Insurance Portability and Accountability Act
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NJCCIC	New Jersey Cybersecurity and Communications Integration Cell
NJOHSP	New Jersey Office of Homeland Security and Preparedness
OT	Operational Technology
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
SCADA	Supervisory Data and Data Acquisition
SDLC	System Development Life Cycle
SOX	Sarbanes-Oxley Act

KEY TERMS

Key terms used throughout this document include the following.

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (SOURCE: CNSSI-4009)

Access Control: The process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities.

Access Control List (ACL): A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

Access Management: A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data – and only using appropriate and controlled methods.

Administrative Safeguards: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information.

Alert: Notification that a specific attack has been directed at an organization's information systems.

Alternate Processing Site: Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed.

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Log: A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

Authenticate: To verify the identity of a user, user device, or other entity.

Authentication: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.

Authenticator: The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Authority: Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere.

Authorization: Access privileges granted to a user, program, or process, or the act of granting those privileges.

Availability: The property of being accessible and useable, upon demand, by an authorized entity.

Baseline Configuration: A set of specifications for a system, or Configuration Item (CI) 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. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Best Practice: A proven activity or process that has been successfully used by multiple enterprises.

Biometric: A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Boundary Protection: Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device: A device with appropriate mechanisms that:

(i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or

(ii) provides information system boundary protection.

Bring Your Own Device (BYOD): Refers to the policy of permitting employees and contractors to use personally owned or third-party owned mobile devices for organizational business purposes.

Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Business Impact Analysis (BIA): An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Change Control: A formal process used to ensure that a process, product, service, or technology component is modified only in accordance with agreed-upon rules. Many organizations have formal Change Control Boards that review and approve proposed modifications to technology infrastructures, systems, and applications. Data Governance programs often strive to extend the scope of change control to include additions, modifications, or deletions to data models and values for reference/master data.

Clear Text: Information that is not encrypted.

Cloud Computing: A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Cloud Service Provider: An entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others.

Compensating Security Control: A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer Emergency Response Team (CERT): Acronym for Carnegie Mellon University's "Computer Emergency Response Team." The CERT Program develops and promotes the use of

appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services.

Confidentiality: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Configuration Management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Contingency Plan: Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Continuity of Operations (COOP) Plan: A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.

Continuous Monitoring: The process implemented to maintain a current security status for one or more information systems, or for the entire suite of information systems, on which the operational mission of the enterprise depends.

Control: A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activates. They can include actions, devices, procedures, techniques, or other measures.

Crisis Management Plan (CMP): Establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms. Communication that occurs within the response phase of emergency-management scenarios. Crisis-management methods of a business or an organization are called a crisis-management plan.

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.

Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Cryptography: The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Data: A subset of information in an electronic format that allows it to be retrieved or transmitted.

Data Privacy: The assurance that a person's or organization's personal and private information is not inappropriately disclosed. Ensuring Data Privacy requires Access Management, eSecurity, and other data protection efforts. (SOURCE: Data Governance Institute)

Data Security: Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Defense-in-Depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Denial of Service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Disaster Recovery Plan (DRP): A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Distributed Denial of Service – (DDoS): A Denial of Service technique that uses numerous hosts to perform the attack.

Embedded System: An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts.

Embedded Technology: Specialized hardware and software that is wholly incorporated as part of a larger system or machine.

Encryption: The process of changing plaintext into ciphertext for the purpose of security or privacy.

Endpoint: Any device capable of being connected, either physically or wirelessly to a network and accepts communications back and forth across the network. Endpoints include, but are not limited to, computers, servers, tablets, mobile devices, or any similar network enabled device.

Entity: Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

Firewall: A gateway that limits access between networks in accordance with local security policy.

Governance: Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

Identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

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 Asset: any data, device, or other component of an information or communications system. Assets generally include hardware (e.g. servers, laptop and desktop computers, switches), software (e.g. commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Classification: A system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability (also classification, information classification, security classification)

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 Technology: The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Integrity: The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Internet: The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share:

a. the protocol suite specified by the Internet Architecture Board (IAB); and
b. the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

Internet of Things (IoT): The network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data.

Intrusion Detection Systems (IDS): Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

Intrusion Prevention Systems (IPS): Hardware or software product that monitors network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

IT Governance: The leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Least Functionality: The principle of least functionality states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary.

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.

Malicious Code: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Media Sanitization: A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Mobile Code: Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Multi-factor Authentication: Authentication using two or more factors to achieve authentication. Factors include:

a. something you know (e.g. password/PIN);
b. something you have (e.g., cryptographic identification device, token); or
c. something you are (e.g., biometric).

Non-Console Access: Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks.

Nonrepudiation: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message.

Operational Technology: The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system.

The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment.

Password: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch Management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Penetration Testing: A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Personally Identifiable Information: Any information about an individual maintained by an agency, including:

(1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and
(2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Personal Identification Number (PIN): A password consisting only of decimal digits.

Personal Information (PI): An individual's first name or first initial and last name linked with any one or more of the following data elements:

1. Social Security number;
2. Driver's license number or State identification card number;
3. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
4. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

Plaintext: Unencrypted information.

Portable Storage Device: An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Privacy: Freedom from unauthorized intrusion or disclosure of information about an individual.

Privileged Account: An information system account with approved authorizations of a privileged user. (SOURCE: CNSSI-4009; NIST SP 800-53)

Privileged User: A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform.

Process: A structured set of activities designed to accomplish a specific objective.

Protocol: Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

Red Team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Remediation: The act of correcting a vulnerability or eliminating a threat.

Remote Access: Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:

1. The conduction of a risk assessment;
2. The implementation of a risk mitigation strategy; and
3. Employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Role-Based Access Control (RBAC): A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Safety: Condition of being protected from harm or other non-desirable outcomes.

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks

posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Requirements: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Sensitive Data: Data that is private, personal, or proprietary and must be protected from unauthorized access.

Sensitive Personally Identifiable Information (SPII): Personal information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Separation of Duties: Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.

Split Tunneling: A computer networking concept that allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application.

Stakeholder: Anyone who has a responsibility for, an expectation from, or some other interest in the enterprise.

Strong Cryptography: Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption and hashing. Examples of industry-tested and accepted standards and algorithms include: AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher).

Strong Password: A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

Supervisory Control and Data Acquisition (SCADA): A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery.

Supply Chain: A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

System: a discrete set of information technologies including computer hardware, software, databases, etc., organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

System Development Life Cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Third Party: Any entity that an organization does business with. This may include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, and agents. Third parties can be both 'upstream' (suppliers and vendors) and 'downstream', (distributors and re-sellers) as well as non-contractual parties.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Trustworthiness: The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

Unauthorized Access: Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.

Unauthorized Disclosure: An event involving the exposure of information to entities not authorized access to the information.

User: Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

User-ID: Unique symbol or character string used by an information system to identify a specific user.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Scan: An automated process to proactively identify security weaknesses in a network or individual system.

Resources and References

NIST - Cybersecurity Framework

NIST – Special Publication (SP) 800-53 Revision 4, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, April 2013

NIST – Special Publication (SP) 800-82, Guide to Industrial Control Systems (ICS) Security, May 2015

NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Revision 1, December 2016.

Center for Internet Security, CIS Controls, Version 7

State of New Jersey Statewide Information Security Manual, March 2018

NJ Board of Public Utilities, Order Docket No. AO16030196, Utility Cyber Security Requirements, March 2016

Cloud Security Alliance, Cloud Controls Matrix, version 3.0.1, October 2017

US CERT - Control System Internet Accessibility, June 2012

US Department of Homeland Security - Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, September 2016

Payment Card Industry, Requirements and Security Assessment Procedures, Version 3.2, April 2016

SANS Secure Architecture for Industrial Control Systems, September 2015.

Purdue University, Purdue Enterprise Reference Architecture, Theodore Williams, 1994