State of Maryland

Cybersecurity & Privacy Glossary

Access Agreements
A formal acknowledgment that individuals understand and accept the rules governing their access to organizational systems and data. (Source: csrc.nist.gov)

Access Control (AC)
The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., buildings, military establishments, border crossing entrances. (Source: csrc.nist.gov)

Accountability
A property that facilitates that the actions of an entity may be traced uniquely to that entity. (Source: NIST SP 800-57 Part 2 Rev 1)

Accounting of Disclosures
Notification that allows individuals to learn who has accessed their Personally Identifiable Information (PII). (Source: NIST SP 800-53 Rev 5)

Adaptive Authentication
A security approach that dynamically adjusts authentication requirements based on contextual risk factors—such as user location, device, behavior, and access patterns. Adaptive authentication enhances traditional login methods by evaluating real-time risk signals and prompting for additional credentials only when necessary—balancing security with user experience. (Source: adapted from Okta and CrowdStrike)

Agency
General term for any department, task force, office, or other entity within the State government to which data governance policy and its standards apply. (Source: DoIT Office of Enterprise Data, Policies and Charters)

Agency Data Owner (ADO)

An individual designated by a State unit to implement measures for the secure, efficient, and effective use of data, provide administrative support to the State Chief Data Officer (SCDO) on behalf of the Agency (or Government Unit). They receive and promptly address inquiries, requests, or concerns about access to the Agency's (unit's) data, comply with direction from the SCDO as to the use and management of the Agency's (unit's) data in accordance with EO 01.01.2021.09. (Source: DoIT Office of Enterprise Data, Policies and Charters)

Application Programming Interface (API)

A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality. (Source: NIST IR 5153)

Artificial Intelligence (AI)

A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. (Source: NIST SP 800-218A)

Artificial Intelligence (AI) Tooling

The set of software, platforms, and technical methods that support the design, development, deployment, and monitoring of artificial intelligence systems across their lifecycle. It encompasses data preparation pipelines, model training frameworks, orchestration platforms, deployment environments, and monitoring solutions that ensure AI systems are scalable, reliable, and compliant with regulatory and organizational requirements. (Source: Adapted from NIST AI RMF 1.0, ISO/IEC 22989:2022)

Assessment

The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. (Source: NIST SP 800-171)

Asset Management

The systematic process of identifying, categorizing, and tracking an organization's information assets, which can include hardware, software, data, personnel, and facilities. (Source: csrc.nist.gov)

Asset Owner

An asset owner is the individual or organizational unit assigned responsibility for the proper management, oversight, and implementation of appropriate controls for an information asset throughout its life cycle. (Source: ISO/IEC 27001)

Attributes

Organization-defined characteristics associated with an account that determine or influence the account's access authorizations, privileges, roles, or security requirements. (Source: DOIT OSM)

Audit Log

A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (Source: csrc.nist.gov)

Audit Record

An individual entry in an audit log related to an audited event. (Source: csrc.nist.gov)

Audit Record Reduction

A process that manipulates collected audit information and organizes it into a summary format that is more meaningful to analysts. (Source: csrc.nist.gov)

Audit Trail

A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result. (Source: NIST SP 800-53 Rev 5)

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (Source: csrc.nist.gov)

Authorization

The right or permission that is granted to a system entity to access a system resource. (Source: NIST SP 800-82 Rev 3)

Authorization to Operate (ATO)

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an

agreed-upon set of security and privacy controls. (Source: NIST SP 800-16 and CNSSI 4009-2015)

Authorization to Operate (ATO) Process

The Maryland State ATO process structured by the State Chief Information Security Officer (SCISO), to operationalize a risk-informed decision framework through which State Authorizing Officials formally approve the deployment and continued operation of an information system within the State's IT ecosystem. (Source: DoIT OSM)

Authorized Access

The level of system or data access granted to an individual based on their role, responsibilities, and successful completion of required security training. (Source: csrc.nist.gov)

Authorizing Official (AO)

A senior agency official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: csrc.nist.gov)

Auto-Forwarding of Emails

A feature of email systems that automatically redirects or sends incoming email messages from one account to another designated email address without requiring manual intervention. (Source: NIST SP 800-45 Rev 2)

Automated Response Mechanism

An automated response mechanism refers to a software-driven capability that detects, analyzes, and initiates predefined actions in response to security events or anomalies—without requiring manual intervention. These mechanisms are typically part of a broader Security Orchestration, Automation, and Response (SOAR) or SIEM platform. (Source: DoIT OSM)

Availability

Ensuring timely and reliable access to and use of information. (Source: csrc.nist.gov)

Awareness Training

The foundational cybersecurity and privacy training program for all personnel. It is designed to help learners understand the roles that they play in protecting information, cybersecurity, and privacy-related assets. It often consists of instructor-led and online courses, exercises, or other methods that inform learners of the acceptable uses of and risks to the organization's systems. (Source: csrc.nist.gov)

Backup

A copy of files and programs made to facilitate recovery if necessary. (Source: csrc.nist.gov)

Behavior Analytics

The act of examining malware interactions within its operating environment including file systems, the registry (if on Windows), the network, as well as other processes and Operating System components. (Source: csrc.nist.gov)

Binding Operational Directive (BOD)

A mandatory instruction requiring specific actions to safeguard Maryland information systems. Each directive is applicable to the State units, or other State-owned network users, identified in the directive. These directives typically address internal cybersecurity practices required to mitigate operational risk; are issued to establish and maintain uniform practices in a specific area of risk; and are generally long-term and remain in effect until officially modified or revoked. (Source: DoIT OSM)

Breach

The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a unit. (Source: MD State Government Code § 10-1305(a)(1)) Where Federal Personally Identifiable Information is involved, the definition of a breach is defined by OMB-17-12.

Business Impact Analysis (BIA)

Process of analyzing operational functions and the effect that a disruption might have on them. (Source: csrc.nist.gov)

Business Continuity Plan (BCP)

The documentation of a predetermined set of instructions or procedures that describes how an organization's mission/business processes will be sustained during and after a significant disruption. (Source: NIST SP 800-34 Rev 1)

Categorization

The process of determining the security category for information or an information system. (Source: csrc.nist.gov)

Center for Internet Security (CIS) Benchmarks

Prescriptive configuration recommendations for various technologies, including operating systems, cloud providers, network devices, and applications. (Source: cissecurity.org)

Certificate Authority (CA)

A trusted entity that issues and revokes public key certificates. (Source: csrc.nist.gov)

Commercial-Off-The-Shelf (COTS) Products

A software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public. (Source: csrc.nist.gov)

Compensating Controls

A safeguard or countermeasure that an organization employs in lieu of a recommended security control. These controls are used when the standard controls are not feasible due to various constraints, such as technical limitations, cost, or operational requirements. The goal is to achieve the same level of security or risk mitigation as the original control. (Source: csrc.nist.gov)

Compiler

A compiler is a specialized software program that translates code written in a high-level programming language (like Python, C++, or Java) into machine code, the low-level instructions a computer's processor can execute directly. (Source: NIST Dictionary of Algorithms and Data Structures)

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Source: NIST SP 800-122)

Configuration Baseline

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. (Source: csrc.nist.gov)

Configuration Control Board (CCB)

A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system. (Source:csrc.nist.gov)

Configuration Item (CI)

Item or aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.(Source: csrc.nist.gov)

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (Source:csrc.nist.gov)

Container

A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container. (Source csrc.nist.gov)

Containment

Limiting the scope and impact of a security incident to prevent further damage. (Source: Microsoft.com)

Contingency Plan (CP)

A contingency plan is a management policy and procedure designed to ensure the continuity of operations for information systems following a disruption. It includes preparation, response, and recovery strategies to restore system functionality and minimize impact. (Source: NIST SP 800-34 Rev 1)

Continuity of Operations Plan (COOP)

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. (Source: NIST SP 800-34 Rev 1)

Continuous Monitoring

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. (Source: NIST SP 800-137)

Control Baseline

The set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk. (Source: csrc.nist.gov)

Core Cyber Response Team (CCRT)

A team made up of representatives from DoIT tasked with the initial assessment of an Information Incident, such as OSM SOC Tier 3, agency privacy personnel, AAG, and DoIT functions such as network, engineering and architecture. The CCRT is responsible for managing and overseeing response activities and for determining if an information incident requires convening the State Incident Response Team. (Source: DoIT OSM)

Cryptographic Agility

The ability to seamlessly update or replace cryptographic algorithms in applications, protocols, and infrastructure without causing operational downtime or compromising security. (Source: NIST CSWP 39)

Criticality Analysis

An end-to-end functional decomposition performed by systems engineers to identify system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions(s). (Source: csrc.nist.gov)

Cybersecurity Supply Chain Risk Management (C-SCRM)

C-SCRM, also referred to simply as Third-Party Risk Management (TPRM), is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. (Source: NIST SP 800-161 Rev. 1)

Data Asset

A digital resource element that has value for an organization, such as databases, documents, files, or datasets, and is managed to support its operations and objectives. (Source: Maryland DoIT Office of Enterprise Data Policies and Glossary)

Data at Rest (DAR)

All data in computer storage media. This includes data on hard drives, backups, and other forms of storage media (Source: NIST SP 800-111)

Data Categorization

Data Categorization is the process of categorizing data based on its sensitivity, value, and the potential impact if it is compromised. This categorization is crucial for determining the appropriate security controls, handling procedures, and access restrictions necessary to protect data through all stages of the data lifecycle. According to the Maryland Data Classification Policy, the four (4) levels of classification are: 1) Public, 2) Protected / Internal-Only, 3) Confidential, and 4) Restricted. (Source: MD Data Classification Policy, 02/21/2025)

Data Classification Level 1

See **State Public Information**.

Data Classification Level 2

See **State Protected Information/Internal Use Only**.

Data Classification Level 3

See **State Confidential Information**.

Data Classification Level 4

See **State Restricted Information**.

Data Custodian

An individual or organization responsible for the safe custody, transport, and storage of data assets. The data custodian maintains the data's quality, security, and

storage according to standards set by the Data Owner. They also implement business rules and ensure proper technical controls are applied to protect the data. (Source: DoIT OED Glossary and Policies)

Data Governance

The exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets with the purpose of ensuring that data is managed properly, according to policies and best practices. (Source: DoIT Office of Enterprise Data, Policies and Charters)

Data Inventory

A catalog of data assets within an organization. It provides information related to the type of data collected, who can access it, where it's stored and how it is used. (Source: DoIT Office of Enterprise Data, Policies and Charters)

Data In Transit (DIT)

Data in transit refers to information traversing a network, whether internal to the organization or external. (Source: NIST SP 800-53 Rev. 5)

Data Loss Prevention (DLP)

A system's ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. (Source: csrc.nist.gov)

Data Matching

An approach that helps organizations identify, consolidate, and protect personal data for accuracy and regulatory compliance.

Data Model

Data model refers to the blueprint of how data is organized, stored, and the relationships and data flow between different data elements. (Source: OED Data Glossary)

Data Owner

A Data Owner is an individual or group responsible for a specific data asset or group of data assets within an Agency. This role requires the owner to act as the primary steward of the data, making crucial decisions regarding its usage, access, and

management. They bear the responsibility for ensuring that data is appropriately classified and handled, in accordance with Federal, State, and Agency Policy as well as the Data Classification Policy, to ensure that appropriate security, privacy protocols, and regulatory compliance controls are rigorously applied to the asset. (Source: DoIT OED forthcoming glossary, consolidated from policies)

Data Retention

The required period during which a data record must be kept and maintained as determined by an approved records schedule, based on legal, fiscal, administrative, and historical value, and ending with either transfer to archives (for permanent records) or destruction (for temporary records). (Source: NARA)

Data Sharing Agreement (DSA)

Internal Data Sharing Agreements (DSA) are for the secure and responsible exchange of data between State Agencies or academic institutions. It outlines the terms and conditions for the secure and responsible exchange of data. It defines the purpose of data sharing, the type of data to be shared, and the responsibilities of each party to protect that data's confidentiality and integrity. See also Data Use Agreement (DUA).

Data Steward

An individual that is responsible for ensuring that organizational information is accurate, consistent, and used properly. Data stewards implement the Federal, State, and Agency data governance policies and are responsible for the quality and integrity of the data on a day-to-day basis. . (Source: DoIT OED forthcoming glossary, consolidated from policies)

Data Use Agreement (DUA)

A DUA is a contract between a State Agency and an external third-party that is given or processes Personal Information (PII) on the State's behalf. NOTE: A DUA is required if an Agency shares data with an external third-party, the data contains PII, and the Data Classification is Level 3 or Level 4. See also Data Sharing Agreement (DSA). (Source: DoIT OED Policies and Charters)

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). (Source: csrc.nist.gov)

Detection and Analysis

The process of identifying potential security incidents and analyzing their nature to determine if they are genuine threats or false positives. (Source: Microsoft.com)

Detection Technology

Tools and techniques used to identify and analyze potential threats, malicious activity, or anomalies within a network or system, enabling organizations to respond quickly and effectively to security incidents.

Digital Media

Digital media includes diskettes, magnetic tapes, removable media, compact discs, digital versatile discs, and removable hard disk drives. (Source: NIST SP 800-53)

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. (Source: NIST SP 800-34 Rev 1)

Disintegration

A physically destructive method of sanitizing media; the act of separating into component parts. (Source: csrc.nist.gov)

Distributed DoS (DDoS)

A denial-of-service technique that uses numerous hosts to perform the attack. (Source: csrc.nist.gov)

Domain Name Service (DNS)

The system by which Internet domain names and addresses are tracked and regulated as defined by IETF RFC 1034 and other related RFCs. (Source: csrc.nist.gov)

Emergency Action Plan (EAP)

A plan developed to prevent loss of national intelligence; protect personnel, facilities, and communications; and recover operations damaged by terrorist attack, natural disaster, or similar events. (Source: csrc.nist.gov)

Emergency Directive (ED)

A mandatory instruction requiring specific actions to address a significant cybersecurity threat, vulnerability, or incident. These directives typically address a specific product, technology or avenue of exploit; and are issued in response to an

immediate or urgent situation that requires prompt action to protect the State, its assets, or its personnel. Usually short-term and in effect only for the duration of the emergency. (Source: DoIT OSM)

Emerging Technologies

Innovations that are still in development or early stages of adoption but have the potential to significantly impact industries and society. These advanced systems and techniques are not yet widely adopted or fully understood. These technologies often require new data governance and policy frameworks to ensure they are used responsibly and ethically in a public service context. Emerging Technologies are often derived from a list of critical and emerging technologies (CETs) maintained by the White House. (Source: adapted from both archives.gov and DoIT OED's Data Readiness Policy)

End-of-Life (EOL)

The point when manufacturer support for software or an asset ceases. (Source: DoIT OSM)

Eradication

The process of eliminating the root cause of the security incident with a high degree of confidence. (Source: Microsoft.com)

Event

Any observable occurrence that involves computing assets, including physical and virtual platforms, networks, services, and cloud environments. Examples of events are user login attempts, the installation of software updates, and an application responding to a transaction request. Many events focus on security or have security implications. Adverse events are any events associated with a negative consequence regardless of cause, including natural disasters, power failures, or cybersecurity attacks. Additional analysis is often needed to determine whether adverse cybersecurity events indicate that a cybersecurity incident has occurred. (Source: NIST SP 800-61r3)

Federal Information Processing Standards (FIPS-140) Certification

U.S. government standard that specifies security requirements for cryptographic modules, which are hardware, software, or firmware components that perform encryption and are used to protect Non-Public information. (Source: csrc.nist.gov)

Federal Risk and Authorization Management Program (FedRAMP)

A governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on security and protection of federal information, and helps accelerate the adoption of secure, cloud solutions. (Source: Fedramp.gov)

Generic Accounts

A user account that is not uniquely assigned to a specific individual. Instead, it's typically used by multiple people who share the same role or function like "reception," "lab user," or "dispatch" and often comes with shared credentials. (Source: DoIT OSM)

Governance

The process of establishing and maintaining a framework and supporting management structure and processes 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. (Source: NIST SP 800-100)

Government Risk and Authorization Management Program (GovRAMP)

A cybersecurity framework that provides a standardized approach to cloud security assessment, authorization, and continuous monitoring for U.S. state, local, tribal, and educational institutions. GovRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 4 framework, modeled in part after FedRAMP, and based on a "complete once, use many" concept that saves time and reduces costs for both service providers and governments. (Source: Govramp.gov)

Group Membership

An organization-defined attribute of an account that identifies the specific security groups to which a user or system account belongs, and which determine the access privileges, roles, and authorizations assigned to that account. (Source: DOIT OSM)

Hardware

A discrete physical component of an information technology system or infrastructure. A hardware device may or may not be a computing device (e.g., a network hub, a webcam, a keyboard, a mouse). (Source: csrc.nist.gov)

Harm

Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaged) or an organization if confidentiality of personal information were breached. (Source: MD DoIT OSM)

High Valued State System (HVSS)

Essential systems, networks, and assets that are vital for the functioning of society and the economy. Their disruption would have significant consequences for public safety, security, health, and economic stability. (Source: DoIT OSM)

Identity

The set of physical and behavioral characteristics by which an individual is uniquely recognizable.(Source: csrc.nist.gov)

Identity Assertions

Identity assertions are statements made by an identity provider (IdP) about a subject (user), typically used in federated identity systems. These assertions convey authentication and attribute information to a relying party (RP), allowing the RP to make access decisions without directly authenticating the user.(Source: csrc.nist.gov)

Identity Proofing

The process of collecting, validating, and verifying a user's identity information for the purposes of establishing credentials for accessing a system. (Source: NIST SP 800-53 Rev 5)

Identity Verification

The process of confirming or denying that a claimed identity is correct by comparing the credentials of a person requesting access with those previously proven and associated with the PIV Card or a derived PIV credential associated with the identity being claimed.(Source: csrc.nist.gov)

Impartiality

Free from conflict of interest related to system development, operation or management. (Source: NIST 800-5 3 Rev 5)

Incident

An event that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Events are observable occurrences, but only those that pose a threat or violate policy rise to the level of (and become) an incident. (Source: MD State definition/ SB812, Ch242)

Incident Response (IR)

The mitigation of violations of security policies and recommended practices. (Source: csrc.nist.gov)

Incident Response Plan (IRP)

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization's information system. (Source: NIST SP 800-34 Rev 1))

Incineration

A physically destructive method of sanitizing media; the act of burning completely to ashes. (Source: csrc.nist.gov)

Independent Assessor

Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of systems. (Source: NIST SP 800-53)

Information Security Continuous Monitoring (ISCM)

Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Note: The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. See organizational information security continuous monitoring and automated security monitoring. (Source: csrc.nist.gov)

Information Security Officer (ISO) Program

The ISO Program is a shared service provided by the Maryland Department of Information Technology (DoIT) to support State agencies in strengthening their cybersecurity posture. The program provides security expertise, guidance, and resources to assist agencies in meeting State and Federal cybersecurity compliance requirements. The service provides agencies with access to experienced cybersecurity professionals who can manage risks, implement security controls, and coordinate incident recovery efforts. (Source: DoIT OSM)

Information Technology (IT)

Any equipment or interconnected system used for automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, firmware, and related resources. IT is often used by executive agencies or contractors under specific contracts. (Source: csrc.nist.gov)

Information User

Often referred to simply as “user”, Any person who interacts with a State computer system, software application, or network service to include State employees, contractors, vendors, third-party providers. (Source: DoIT OSM)

Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (Source: csrc.nist.gov)

Insider Threat

The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. (Source: NIST SP 800-171r3)

Integrity (of data)

Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. (Source: csrc.nist.gov)

International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard. (Source: ISO.org)

Internet of Things (IOT)

User or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances. (Source: csrc.nist.gov)

Least Privilege

A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.(Source: csrc.nist.gov)

Log Retention

Archiving logs on a regular basis as part of standard operational activities. (Source: NIST SP 800-92)

Machine Learning (ML)

The development and use of computer systems that adapt and learn from data with the goal of improving accuracy. (Source: NIST SP 800-55v1)

Macro-Segmentation

Macro-segmentation, or traditional network segmentation, involves dividing the network into large, coarse-grained segments based on broad criteria like function, location, or department. (Source: adapted from Checkpoint, Crowdstrike)

Malware

Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (Source: csrc.nist.gov)

Managed Interface

An interface within an information system that provides boundary protection capability using automated mechanisms or devices. (Source: csrc.nist.gov)

Matching Program

A matching program is a computerized comparison of records from two or more automated Privacy Act systems of records, or an automated system of records and automated records maintained by a non-Federal agency (or agent thereof). (Source: csf.tools)

Melting

A physically Destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat. (Source: csrc.nist.gov)

Metadata

Form of data that describes other data, including attributes such as what data an organization has, what it represents, how it is classified, where it came from, how it moves within the organization, how it evolves through use, who can and cannot use it, and whether it is of high quality. (Source: DoIT OED Policies)

Micro-Segmentation

A security technique that creates fine-grained network segments to isolate specific workloads, devices, or even individual applications, limiting lateral movement and enforcing least-privilege access. (Source: adapted from VMware and Palo Alto Networks)

Mission Essential Functions

The critical activities that an organization must perform to achieve its core objectives, even during emergencies or disruptions. (Source: NIST SP 800-34 Rev 1)

Mobile Code

Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. (Source: csrc.nist.gov)

Mobile Device

A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local,

non-removable data storage; and (iv) is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. (Source: csrc.nist.gov)

Multi-Factor Authentication (MFA)

Authentication that uses two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). (Source: csrc.nist.gov)

National Institute of Standards for Technologies (NIST)

The US Department of Commerce's National Institute of Standards for Technologies is responsible for coordinating Federal, State, and local documentary standards and conformity assessment activities. (Source: nist.gov)

Near-Real-Time

The ability to capture and assess security-related information as frequently as needed to support risk-based decisions. (Source: NIST SP 800-137)

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. (Source: csrc.nist.gov)

Network Access

Any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. (Source: DoIT OSM)

NIST Cyber Security Framework (CSF)

A framework designed by the National Institute of Standards & Technology (NIST) to help organizations manage and reduce cybersecurity risks using a flexible and

comprehensive approach to improving cybersecurity practices across industries, regardless of size or sector. (Source: NIST CSF 2.0)

Non-Digital Media

Non-digital media includes paper and microfilm. (Source: NIST SP 800-53)

Non-Human Identities (NHI)

Also referred to as Non-Person Entity (NPE), this is an entity with a digital identity that acts in cyberspace but is not a human actor. Examples include organizations, hardware devices, software applications, and information artifacts. (Source: CNSSI 4009-2015)

Non-Organizational User

These are users who are not organizational users, including public users.

Offload

The method of reducing the attack surface by moving non-essential functions to separate systems or external providers (not co-locating).

Operational Technology (OT)

Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (Source: csrc.nist.gov)

Organizational User

These are employees or individuals considered by the organization to have equivalent status, including contractors and guest researchers. (Source: NIST SP 800-53 Rev 5)

Organizationally Defined Parameter (ODP)

The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a predefined list provided as part of the control or control enhancement. See assignment operation and selection operation. (Source: NIST SP 800-53 Rev 5)

Overlay

A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.(Source: csrc.nist.gov)

Passwordless Authentication

Passwordless authentication verifies user identities without passwords or other knowledge-based factors or information. Instead, the security team verifies a user's identity using either a "something-you-have" type of authentication factor, which is an object that uniquely identifies the user (e.g. a mobile passkey or hardware security key) or a "something-you are" type of factor (e.g. biometrics, including a fingerprint or facial scan). (Source: RSA.com)

Patch

A patch is an update to an operating system, application, or other software issued specifically to correct particular problems, such as a security vulnerability or a stability issue. (Source: NIST 800-40 Rev 4)

Peer-to-peer (P2P) File Sharing

Peer-to-peer (P2P) networking allows computers to share resources directly with each other, such as files or disk storage, without requiring a central server. (Source: NIST SP 800-101 Rev 1)

Penetration Testing

A method of testing, sometimes referred to as pentesting, where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resource. (Source: NIST SP 800-95)

Personal Information

An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

(i) a Social Security number;

(ii) a driver's license number, state identification card number, or other individual identification number issued by a unit;
(iii) a passport number or other identification number issued by the United States government;
(iv) an Individual Taxpayer Identification Number; or
(v) a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

(Source: MD State Government Code § 10-1301(c)(1)) This data falls under confidential data (Data Classification Level 3) in accordance with the State Data Classification Policy.

Personally Identifiable Information (PII)

Information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric data records. either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). (Source: OMB-17-12)

Phishing

A technique for attempting to acquire protected personal or financial data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person. (Source: csrc.nist.gov)

Ping Flood Attack

A flood attack occurs when the attacker sends a large volume of traffic, often using protocols such as ICMP, to overwhelm the target's network resources, thereby causing a denial of service. (NIST SP 800-61 Rev 2)

Plan of Action & Milestones (POA&M)

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for meeting the tasks, and scheduled milestone completion dates. (Source: csrc.nist.gov)

Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages,

libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (Source: csrc.nist.gov)

Preparation

Establishing the necessary infrastructure, policies, and procedures to effectively respond to cybersecurity incident (Source: csrc.nist.gov)

Pretexting

Attackers use a fictional backstory to manipulate a victim into revealing sensitive information or influence behavior. (Source: Carnegie Mellon University)

Principle of Least Privilege

The principle is that users and programs should only have the necessary privileges to complete their tasks. (Source: csrc.nist.gov)

Privacy Act

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. (Source: justice.gov)

Privacy Incident

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an unauthorized purpose. (Source: NIST Privacy Framework)

Privileged Access

Access to perform security-relevant functions that ordinary users are not authorized to perform, requires additional training, and must sign an acceptable use policy. (Source: NIST 800-50r1)

Privileged Accounts

An information system account with approved authorizations of a privileged user. (Source: csrc.nist.gov)

Public Key Infrastructure (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. (Source:csrc.nist.gov)

Pulverization

A physically destructive method of sanitizing media; the act of grinding to a powder or dust. (Source: csrc.nist.gov)

Quid Pro Quo

Something given or received for something else. An example is an attackers lures users with incentives to acquire information. (Source: Merriam-Webster)

Real-Time Monitoring

The delivery of continuously updated data about systems, processes or events. (Source: Techtarget.com)

Real-Time Risk Assessment

Real-time risk assessment refers to the continuous evaluation of contextualized risk data to improve situational awareness and prioritize required actions—supporting ongoing authorization and dynamic decision-making. (Source: NIST Cyber Risk Scoring Program)

Reconstitution

The process of restoring normal operations after a disruption or emergency.

Recovery

Developing and implementing plans and activities to restore capabilities or services impaired by a cybersecurity incident, ensuring timely recovery to normal operations and improving resilience. (Source: csrc.nist.gov)

Recovery Point Objective (RPO)

The point in time to which data must be recovered after an outage. (Source: NIST SP 800-34 Rev 1)

Recovery Time Objective (RTO)

The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes. (Source: NIST SP 800-34 Rev 1)

Remanence

Residual information that remains in the storage media after clearing. (Source: CNSSI 4009-2015)

Removable Media

Portable data storage medium that can be added to or removed from a computing device or network. Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, east, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD). See also portable storage device. (Source: csrc.nist.gov)

Resilience

The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. (Source: csrc.nist.gov)

Restoration

The process of changing the status of a suspended (i.e., temporarily invalid) certificate to valid. (Source: csrc.nist.gov)

Risk Acceptance

The decision to accept a certain level of residual risk after implementing necessary controls. This means the organization acknowledges the potential impact of the risk but determines that it falls within their risk tolerance or appetite. Essentially, they choose not to take further action to mitigate or transfer the risk. (Source: csrc.nist.gov)

Risk Assessment Report (RAR)

The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk. (Source: csrc.nist.gov)

Risk Avoidance

A strategy to eliminate risk by not engaging in activities or operations that could lead to potential threats. Essentially, it involves making decisions to avoid actions or situations that could expose an organization to risk. (Source: csrc.nist.gov)

Risk Framing

The set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk. (Source: csrc.nist.gov)

Risk Management

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (Source: csrc.nist.gov)

Risk Mitigation

The process of prioritizing, evaluating, and implementing appropriate controls or countermeasures to reduce risk to an acceptable level. This involves addressing vulnerabilities, threats, and potential impacts identified during the risk management process. (Source: csrc.nist.gov)

Risk Response

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: csrc.nist.gov)

Risk Transference

A strategy where an organization shifts the impact of a risk to another entity, often through mechanisms like insurance or outsourcing. This approach is part of the broader risk response strategies outlined by NIST, which also include accepting, avoiding, mitigating, and sharing risks. (Source: csrc.nist.gov)

Role-Based Training

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the cybersecurity and privacy roles defined. (Source: csrc.nist.gov)

Root Cause Analysis

A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. (Source: csrc.nist.gov)

Safeguards

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. (Source: csrc.nist.gov)

Safeguard Computer Security Evaluation Matrix (SCSEM)

Structured assessment tools used to evaluate the security of IT environments that handle sensitive information. They help agencies achieve compliance with IRS Publication 1075, which outlines security requirements for protecting taxpayer data. (Source: irs.gov)

Sanitization

Process to remove information from media such that information recovery is not possible. (Source: csrc.nist.gov)

Secure Access Service Edge (SASE)

A cloud-delivered architecture that combines wide-area networking (WAN) capabilities with network security functions (such as ZTNA, CASB, SWG, and FWaaS) into a unified service delivered at the edge. It enables organizations to provide secure, consistent, and optimized access to applications and data for users regardless of location (Source: microsoft.com)

Secure Shell (SSH)

A network protocol that provides strong authentication and secure communications over insecure channels. (Source: NIST SP 800-153)

Security and Privacy Awareness

The ongoing process of informing personnel about cybersecurity and privacy risks, organizational policies, and best practices to maintain a secure environment. (Source: csrc.nist.gov)

Security Function

The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. (Source: NIST SP 800-53 Rev 5)

Security Baseline

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. (Source: csrc.nist.gov)

Security Control

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. (Source: csrc.nist.gov)

Security Event

Any observable occurrence in a network or system. (Source: csrc.nist.gov)

Security Incident

An event that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. Events are observable occurrences, but only those that pose a threat or violate policy rise to the level of (and become) an incident. (Source: MD State definition/ SB812, Ch242)

Security Incident Response Team (SIRT)

A cross-functional team made up of leaders across DoIT and other functions within agencies across the State who are trained in how to prepare for, manage and respond to information incidents. Depending on the details and circumstances of the specific information incident, relevant SIRT members will be required to participate in the response effort. (Source: DoIT OSM)

Sensitive Data

Personal data that includes data revealing racial or ethnic origin, religious beliefs, consumer health data, sex life, sexual orientation, status as transgender or nonbinary, national origin, or citizenship or immigration status, genetic data or biometric data, personal data of a consumer that the controller knows or has reason to know is a child, or precise geolocation data. This data is subcategory of personal data which falls under confidential data (Data Classification Level 3) in

accordance with the State Data Classification Policy. (Source: Maryland Code §14-4701).

Separation of Duties (SoD)

The principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time). An example of dynamic separation of duty is the two-person rule. The first user to execute a two-person operation can be any authorized user, whereas the second user can be any authorized user different from the first.(Source: csrc.nist.gov)

Service Account

A non-human digital identity used by applications, scripts, and machines to perform tasks and communicate with other systems, rather than by a person. These privileged accounts allow automated processes, like database backups or API calls, to access resources securely, running behind the scenes to keep IT infrastructure and services functioning efficiently and automatically. (Source: DoIT OSM)

Service Provider

A provider of basic services or value-added services for operation of a network; generally, refers to public carriers and other commercial enterprises. (Source: csrc.nist.gov)

Shared Accounts

An information system account that is used by multiple individuals. (Source: NIST SP 800-53 Rev. 5)

Shredding

A method of sanitizing media; the act of cutting or tearing into small particles. (Source: csrc.nist.gov)

Smurf Attack

a distributed denial of service (DDoS) attack in which ICMP echo request packets with a spoofed source address are sent to a broadcast address. Systems on the network respond to the spoofed address, overwhelming the target system with traffic. (Source: NIST SP 800-61 Rev 2)

Social Engineering / Social Mining

The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust. Social mining aims to gather information for future attacks. (Source: NIST SP 800-63-3)

Software

A collection of computer programs and associated data that may be dynamically written or modified during execution. (Source: csrc.nist.gov)

Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (Source: csrc.nist.gov)

State Confidential Information

Information that is protected from either release or disclosure by law and classified as confidential (Data Classification Level 3) in accordance with the State Data Classification Policy. Confidential information includes but is not limited to Personal Information, Personally Identifiable Information (PII), Protected Health Information (PHI), credit card and financial information, student records, information about children, and other privileged or sensitive information. (Source: Source: DoIT OSM)

State Data

All data created or in any way originating with a Unit of State government, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, a service provider's hardware, or exists in any system owned, maintained or otherwise controlled by the State or by a service provider. (Source: DoIT OSM)

State Confidential Information

Data that is determined to be classified as Protected/Internal Use Only (**Data Classification Level 3**) in accordance with the State Data Classification Policy. Information that is protected from either release or disclosure by law. (Source: MD Data Classification Policy)

State Non-Public Information

Any information that is determined to be classified as either protected/internal use only, confidential, or restricted (**Data Classification Level 2 or above**) in accordance with the State Data Classification Policy. (Source: MD Data Classification Policy)

State Protected Information/Internal Use Only

Data that is determined to be classified as Protected/Internal Use Only (**Data Classification Level 2**) in accordance with the State Data Classification Policy. Data within this classification is accessible to Agency personnel or contractors who require access, and require protection from unauthorized use, disclosure, modification, or destruction. (Source: MD Data Classification Policy)

State Public Information

Data that is determined to be classified as public (**Data Classification Level 1**) in accordance with the State Data Classification Policy. Public data is data that a State entity has collected or created and is permitted, required or able to make available to the public consistent with applicable laws, rules and regulations. (Source: MD Data Classification Policy)

State Restricted Information

Data that is determined to be classified as restricted (**Data Classification Level 4**) in accordance with the State Data Classification Policy. Restricted is data that, if disclosed, accessed, altered or destroyed without authorization, could cause significant damage to the Agency (e.g., financial loss), damage to the Agency's or the State's reputation, or the individual(s) whose information is compromised, and may lead to criminal charges or other legal consequences. (Source: DoIT OSM)

State System

An information system owned, operated, or maintained by any Unit of State government with the Executive Branch of the State of Maryland (hereafter referred to as "agency"). These systems include those used or operated by an agency, a

contractor of an agency, or another organization on behalf of an agency. This definition encompasses a broad range of systems, from simple computer systems to complex networks and databases, used to manage and process information for State government operations. This definition applies to any system used to collect, process, store, transmit, or disseminate digital information for State purposes. (Source: DoIT OSM)

Supply Chain

Linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle. (Source: csrc.nist.gov)

Syn Flood Attack

A SYN flood occurs when an attacker sends a succession of TCP SYN requests to a target system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. (Source: NIST SP 800-61 Rev 2)

System Account

An information system account with the authorizations of a privileged user, used by an operating systems or application to perform system-level functions. (Source: NIST SP 800-171)

System and Organization Control (SOC) 2 Type 2

SOC 2 Type 2 is an independent audit report that evaluates not only the design of an organization's security controls but also their operational effectiveness over a defined period of time (typically 3–12 months). It is based on the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria (TSC): Security, Availability, Processing Integrity, Confidentiality, and Privacy. SOC 2 Type 2 provides assurance to customers and stakeholders that the organization consistently protects sensitive data and maintains compliance standards. Unlike SOC 2 Type 1, which is a point-in-time assessment, SOC 2 Type 2 demonstrates ongoing reliability and effectiveness of controls in practice. (Source: AICPA)

System Development Life Cycle

The scope of activities associated with a system, encompassing the initiation, development, acquisition, implementation, operation, and maintenance of the system. (Source: NIST 800-64)

System Information Exchange

When two or more systems share data. (Source: NIST SP 800-13r5)

System Owner

A person or organization that has responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. (Source: NIST SP 800-53)

System Security & Privacy Plans

Formal document that provides an overview of the security and privacy requirements for an information system and describes the security and privacy controls in place or planned for meeting those requirements. (Source:csrc.nist.gov)

Tailgating

Also known as piggybacking, is a physical security breach where an unauthorized individual gains access to a restricted area by closely following an authorized person, often by exploiting social engineering tactics. (Source: csrc.nist.gov)

Tailoring

The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements. (Source: csrc.nist.gov)

Tampering

An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data. (Source: csrc.nist.gov)

Teardrop Attack

A type of denial-of-service attack that involves sending fragmented IP packets that are designed to overlap each other when reassembled. Some operating systems fail to properly handle these overlapping fragments, causing system crashes or instability. (Source: NIST SP 800-61 Rev 2)

Third Party Providers (or Vendors)

Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system. (Source: csrc.nist.gov)

Third Pary Risk Management (TPRM)

TRRM, also referred to as Cybersecurity Supply Chain Risk Management (C-SCRM), is a systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. (Source: NIST SP 800-161 Rev)

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 for a threat-source to successfully exploit a particular information system vulnerability. (Source: csrc.nist.gov)

Threat Awareness Program

A program that includes a cross-organization information-sharing capability for threat intelligence. (Source: csrc.nist.gov)

Transport Layer Security (TLS)

Authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS. (Source: csrc.nist.gov)

Unit of State Government

An agency or unit of the Executive Branch of State government. (Source: Maryland Code, State Finance and Procurement § 3.5-101)

U.S. Computer Emergency Readiness Team (US-CERT)

A partnership between the Department of Homeland Security (DHS) and the public and private sectors, established to protect the nation's internet infrastructure. (Source: csrc.nist.gov)

Uninterruptible Power Supply (UPS)

A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost. (Source: csrc.nist.gov)

Virtual Machine

A software-defined complete execution stack consisting of virtualized hardware, operating system (guest OS), and applications. (Source: csrc.nist.gov)

Virtual Private Network (VPN)

Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line. (Source: csrc.nist.gov)

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Source: csrc.nist.gov)

Vulnerability Disclosure Program (VDP)

A structured framework that allows individuals, often ethical hackers or security researchers, to report security vulnerabilities they discover in an organization's systems (Source: cisa.gov)

Wiping

Overwriting media or portions of media with random or constant values to hinder the collection of data. (Source: csrc.nist.gov)

Zero Trust Architecture (ZTA)

An integrated cybersecurity approach that replaces static, network-based perimeters with continuous verification of users, assets, and resources. No entity is implicitly trusted; access is granted based on dynamic risk, least privilege, and continuous monitoring to ensure only authorized and validated activities occur within State systems. (Source: adapted from NIST SP 800-207)

Zero Trust Network Access (ZTNA)

A security model and service that provides secure, adaptive, and segmented access to applications and resources based on identity, device posture, and context policies. It enforces the principles of verify explicitly, least privilege, and assume breach, ensuring that every access request is continuously authenticated and authorized regardless of user location, device, or network. (Source: adapted from Microsoft/Cisco)