Glossary

Version Version 12 · Published January 15, 2026 · Glossary of Terms

"Access Control": 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., federal buildings, military establishments, border crossing entrances). [*Source:* FIPS 201-3]

"Administrator Account": An account with full/elevated privileges on a computer/ device, system, or application.

"Algorithm": A clearly specified mathematical process for computation derived from a set of rules that, if followed, will give a prescribed result. [*Source:* NIST SP 800-107 Rev. 1]

"Approved Hardware (End User Device) List": A documented and vetted list of models and specifications for end user devices that meet the enterprise's performance, security, and supportability criteria.

"Artificial Intelligence (AI)": Technologies that encompass a variety of techniques and approaches, such as machine learning, natural language processing, computer vision, and robotics, aimed at enabling machines to perform tasks that typically require human intelligence. For the sake of clarity, AI does not include traditional data science activities or robotic process automation.

"**Audit Log":** A chronological record of system activities. Includes records of system access and operations performed in a given period. [*Source:* CNSSI 4009-2015]

"**Audit Trail":** A record showing who has accessed an information technology (IT) system and what operations the user has performed during a given period, including 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 final result. [*Source:* CNSSI 4009-2015]

"Authentication": The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system. This process ensures that someone's identity or the validity of something to ensure that only authorized users can access information, systems, or other resources. [*Source:* NIST SP 800-53 Rev. 5]

"Authorization": The right or permission (access privileges) that is granted to a user, program, or process (system entity) to access a system. [*Source:* NIST SP 800-82r3]

"Authorization to Operation (ATO)": The official management decision given by a senior official to authorize operation of a system or the common controls inherited by designated organizations systems and to explicitly accept the risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Also known as authorization to operate. [*Source:* NIST SP 800-12 Rev. 1]

"**Availability":** Ensuring timely and reliable access to and use of information. [*Source:* CNSSI 4009-2015 from 44 U.S.C., Sec. 3542(b)(1)(c)]

"**Baseline Configurations":** 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. Baseline configurations establish a known and secure state for an information system and serve as the foundation for future builds, updates, and configuration changes. [*Source:* CNSSI 4009-2015]

"**Biometric Data":** Biological attribute of an individual from which distinctive and repeatable values can be extracted for the purpose of automated recognition. Fingerprint ridge structure and face topography are examples of biometric characteristics. [*Source:* FIPS 201-3 from ISO/IEC 2382-37;2017]

"Breach": The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, or where authorized users take actions for an other than authorized purposes, have access or potential access to sensitive information, whether physical or electronic. [*Source:* NIST SP 800-175A]

"**Certificate Authority":** A trusted entity that issues and revokes public key certificates. [*Source:* NISTIR 8149]

"**Change Advisory Board (CAB)":** A formally designated group of stakeholders responsible for reviewing, approving, and prioritizing changes to configuration items (e.g., hardware, software, firmware), and documentation throughout the development and operational life cycle of an information system. CABs may be organized into multiple tiers based on impact and scope. [*Source:* NIST SP 800-128]

"**Change Control Database (CCDB)":** The system of record used to document, track, and manage configuration changes and associated approvals throughout the system lifecycle.

"**Change Management":** The systematic proposal, justification, implementation, testing, review, and disposition of system changes, including upgrades and modifications. It involves managing and monitoring configurations of information systems to achieve adequate security and minimize organizational risk while supporting business functionality.

"**Change Manager":** Designated role responsible for overseeing the change management process, including coordination of CAB activities and enforcement of baseline risk requirements compliance.

"**Confidentiality":** Preserving unauthorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [*Source:* FIPS under 'confidentiality' from 44 U.S.C., Sec. 3542]

"**Configuration Item":** Any component of an information system, including hardware, software, documentation, or service, treated as a single entity and that is subject to configuration management and change control. [*Source:* CNSSI 4009-2015]

"Configuration Management Plan (CMP)": A comprehensive plan providing guidelines for establishing, maintaining, and monitoring secure configurations of information systems to enhance security and minimize risks. [*Source*: NIST SP 800-128]

"**Contingency Plan":** A written plan 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 (DRP) for major disruptions. [*Source:* CNSSI 4009-2015]

"**Continuous Monitoring":** Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This includes the use of automated procedures to ensure security controls are not circumvented or the use of these tools to track actions taken by subjects suspected of misusing the information system. [*Source:* CNSSI 4009-2015 from NIST SP 800-137]

"**CyberGUARD":** A State of Iowa enterprise information security program that encompasses a variety of risk products, including the establishment of baseline risk requirements, policies, procedures, directives, and other risk-related documents. CyberGUARD stands for Cyber Governance, Understanding, Assessment, and Risk Directive. The programs intent is to provide a robust framework or resources for managing cybersecurity risks across the enterprise.

"**Data":** A subset of information in an electronic format that allows it to be retrieved or transmitted. [*Source:* NIST SP 1800-10]

"**Digital Certificate":** A set of data that uniquely identifies a public key that has a corresponding private key and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information and is digitally signed by a certification authority (i.e., a trusted party), thereby binding the public key to the owner. [*Source:* FIPS 204]

"**Digital Signature":** A digital representation of a signature that provides assurance of the origin, authenticity, and integrity of the data. It is generated through a cryptographic transformation and is used to verify the identity of the signer and ensure that the information has not been altered. [*Source:* FIPS 186-5 under 'digital signature']

"DOM Workers": All employees, contractors, vendors, interns, board members, and any individual working for the Iowa Department of Management who has access to State of Iowa-managed systems or information, or performs Information Technology ("IT") or Criminal Justice Information ("CJI") work for DOM.

"Draft Information Security Policy": High-level statement establishing minimum requirements for decision-making and behavior. Internal only and not enforceable. Requires review and approval to proceed to another policy state – interim or final.

"Due Care": The reasonable steps or action an organization takes to protect its information assets from unauthorized access, use, disclosure, modification, or destruction. It involves implementing necessary precautions to ensure compliance with industry best practices and maintaining a robust cybersecurity posture. Key aspects of due care include establishing comprehensive information security policies, conducting regular audits, and providing ongoing cybersecurity training for employees. [*Source:* NIST SP 1326]

"Due Diligence": The practice of taking reasonable, risk-based measures to safeguard an organization's assets, information, finances, and reputation. It involves proactively identifying, assessing, and mitigating risks to ensure compliance with applicable laws, regulations, and standards (e.g., NIST, federal mandates). Due diligence encompasses implementing appropriate security controls, validating third-party relationships, and maintaining continuous oversight to protect confidentiality, integrity, and availability of systems and information. It reflects a commitment to responsible stewardship and accountability in managing public resources and trust. [*Source:* Aligns with NIST RMF and FISMA]

"Emergency Configuration Change": A configuration change that must be implemented urgently to address critical issues such as security incidents or outages, following an expedited approval process and post-implementation review.

"Encryption": Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. [*Source:* NIST SP 800-82r3 under Encryption from RFC 4949 - adapted]

"End-User Device": Tangible computing devices designed for individual users to interact with, capable of storing data, and connecting to networks.

"Enterprise Workers": All employees, contractors, vendors, interns, board members, and any individual working for the Iowa Department of Management or any Supported Entity (Iowa Code Chapter 8) who has access to State of Iowa-managed systems or information, or performs Information Technology ("IT") or Criminal Justice Information ("CJI") work for DOM or any Supported Entity.

"Final Information Security Policy:" Long-term
strategy establishing minimum requirements for decision-making and behavior. Enforceable. Requires review and approval.

"**Firewall":** A gateway that limits access between networks in accordance with local security policy. [*Source:* CNSSI 4009-2015]

"Foundational Information Security and Privacy Awareness and Training": The purpose of this type of training is for the participant to gain a basic understanding of the need for information security and privacy and the actions that the individual can take to maintain security and privacy and respond to suspected incidents. This training also increases awareness regarding the importance of operations security.

"Generative Artificial Intelligence": A type of Artificial Intelligence that generates content such as text, images, audio, and video. [*Source:* NIST SP 800-218A]

"Hardened Token": A security token that is physically secure and difficult to replicate or bypass. Generally, they are hardware devices
that utilize encryption algorithms and can include features like biometrics or secure PINs to complete two-factor authentication (2FA) or multi-factor authentication (MFA). [*Source:* NIST SP 800-63-1]

"Identification": The process of discovering the identity of a person or item from a collection of similar entities. It involves verifying the identity of a user, process, or device which is crucial for granting access to resources in an IT system. Identification is part of a broader framework that includes authentication, which verifies the validity of the claimed identity. [*Source:* CNSSI 4009-2015
NIST SP 800-79-2 under Identification]

"Incident": An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information

that the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation: of security policies, security procedures, or acceptable use policies. [*Source:* FIPS 200 under ’ incident’]

"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. An instance of an information type. [*Source:* NIST SP 800-31 Rev 1 under ’information’ from CNSSI 4009, FIPS 199]

"Information (Data) Custodian": A technical role, assigned to an individual or team, rooted in IT operations. Custodians are responsible for the secure storage, protection, and technical integrity of information assets. Their duties include implementing and maintaining infrastructure (databases, storage systems), enforcing security and privacy controls (encryption, access management, logging), managing backups, and ensuring compliance with regulatory frameworks such as NIST, GDPR, CCPA, and FISMA. They focus on availability, confidentiality, and integrity at the system level, serving as the technical foundation for data governance. [*Source:* Definition based on industry standards, specifically NIST and FISMA]

"Information (Data) Owner": Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [*Source:* CNSSI 4009]

"Information Privacy": The safeguarding of human autonomy and dignity through various means, including confidentiality, predictability, manageability, and disassociability. [*Source*: NIST SP 800-50r1]

"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. [*Source:* FIPS 200 under ’information security’ from 44 U.S.C., Sec. 3542]

"Information Spillage": Security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. [*Source:* CNSSI 4009-2015 under ’classified information spillage’]

"Information (Data) Steward": Individual or team responsible for the management and oversight of information. Stewards are focused on the quality, usability, and governance of data. Stewards define and enforce business rules, maintain metadata, and ensure data accuracy, completeness, and consistency across systems. They document data for accessibility, set access policies aligned with organizational objectives, and collaborate with custodians to balance compliance with business value. Their goal is to transform data into a strategic asset that

supports decision-making and regulatory adherence. [*Source:* CNSSI 4009 and NIST industry standards]

"Information System": A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [*Source*: FIPS 200 under 'information system' from 44 U.S.C., Sec. 3502]

"Information Technology (IT) Resources": Collectively includes data, information, information systems, technology, and resources.

"Integrity": Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [*Source:* NIST SP 800-59 under 'integrity' from 44 U.S.C., Sec. 3542(b)(1)(A)]

"Interim Information Security Policy": High-level statement establishing minimum requirements with transitional steps toward a final policy. Enforceable. Requires review and approval.

"Local Logon": Access to an organizational system by a user (or process acting on behalf of a user) through a direct connection without the use of a network. This means that the user is accessing the system directly, without going through any intermediary network. [*Source:* CNSSI 4009-2015]

"Malicious Code": Software or firmware intended to perform an unauthorized process that will have adverse impacts on the confidentiality, integrity, or availability of a 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. [*Source:* NIST SP 800-53 Rev. 5]

"Malware": Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. [*Source:* CNSSI 4009-2015]

"Multi-Factor Authentication (MFA)": Authentication using 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*: CNSSI 4009-2015 under 'multifactor authentication']

"Non-Local Logon": The process of logging into a system or application where authentication occurs via a networked system, such as a domain controller, cloud-based authentication provider, or VPN. This includes remote logons and on-premise authentication to shared resources that require verification from an external identity service.

"Non-Local Maintenance": Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. [*Source:* CNSSI 4009-2015]

"Non-Repudiation": A service that is used to provide assurance of the integrity and origin of information in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (e.g., the signatory). [*Source*: FIPS 186-5 under 'non-repudiation']

"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. [*Source:* CNSSI 4009-2015]

"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:* FIPS 201-3 under 'personally identifiable information (PII)' from OMB M-17-12- adapted]

"Phishing": A technique for attempting to acquire sensitive information and 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:* CNSSI 4009-2015]

"Planned Configuration Change": A non-emergency change that requires formal assessment, scheduling, review, and approval prior to implementation.

"Policy": Statements, rules or assertions that specify the correct or expected behavior of an entity. Policy defines what must be done and sets clear goals, acceptable behaviors, and minimum risk thresholds for workforce members. [*Source:* NIST SP 800-95 from Open Grid Services Architecture Glossary of Terms]

"Pre-authorized Configuration Change (Standard)": A low-risk, well-understood change that has a predefined process for implementation and does not require full CAB review for approval.

"Principle of Least Privilege (PoLP)": 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:* NIST SP 800-53, Rev 5 from CNSSI 4009-2015]

"Privileged Account": A user that is authorized (and, therefore, trusted) to perform system and application functions that ordinary users are not authorized to perform. [*Source:* CNSSI 4009-2015]

"Procedure": Specified way to carry out an activity or a process with detailed, repeatable instructions that align with policy objectives (e.g., technical solutions). It can complement a policy by detailing how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. [*Source:* ISO 9000:2015 Quality management systems]

"Production Environment (Environment of Operation)": The physical, technical, and organizational setting in which an information system operates, including but not limited to: missions/business functions; mission/business processes; threat space; vulnerabilities; enterprise and information security architectures; personnel; facilities; supply chain relationships; information technologies; organizational governance and culture; acquisition and procurement processes; organizational policies and procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs). [*Source:* CNSSI 4009-2015 from NIST SP 800-30 Rev. 1]

"Protected Data": Information in any form, including physical, electronic (digital), or spoken information or data that is protected by state or federal law, industry specific mandates, or that is attributed to the confidentiality, integrity, and availability of state of Iowa's resources.

"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. Framework established to issue, maintain, and revoke public key certificates. [*Source:* CNSSI 4009-2015]

"Remediation": The neutralization or elimination of a vulnerability or the likelihood of its exploitation. [*Source:* NIST SP 800-216]

"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). [*Source:* NIST SP 800-128]

"Removable Storage Device": Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. Note: Examples include, but are not limited to: USB flash drives, external hard drives, and external solid-state disk (SSD) drives. Portable Storage Devices also include memory cards that have additional functions aside from standard data storage and encrypted data storage, such as built-in Wi-Fi connectivity and global positioning system (GPS) reception. May also be referred to as removable media. [*Source:* CNSSI 4009-2015]

"Risk": A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [*Source: NIST SP 800-30 Rev. 1]*

"Risk Assessment": The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [*Source:* NIST SP 800-137 under Risk Assessment from CNSSI 4009]

"Role-Based Security and Privacy Awareness Training": Role-based training strives to produce relevant and needed security and privacy knowledge and skills within the workforce. Role-Based Security and Privacy
Training supports competency development and helps personnel understand and learn how to better perform their specific security or privacy role, which ultimately achieves more secure and protected information and systems.

"Root Certificate Authority": In a hierarchical public key infrastructure (PKI), the certification authority (CA) whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. [*Source:* CNSSI 4009-2015]

"Sanitize": Actions taken to render information written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. [*Source:* NIST SP 800-172]

"Security Categorization": The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems. [*Source:* NIST SP 800-137 under 'security categorization' from CNSSI 1253, FIPS 199]

"**Sensitive Information":** Information that could adversely affect the national interest, federal or state programs, organizational or enterprise interests, or individual privacy (e.g., confidential). This includes data that can be used to distinguish or trace an individual's identity or any information requiring protection based on data criticality and system value.

"Separation of Duty (SOD)": Refers to 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 [R.S. Sandhu., and P Samarati, “Access Control: Principles and Practice,” IEEE Communications Magazine 32(9), September 1994, pp. 40-48.]. There are various types of SOD, an important one is history-based SOD that regulate for example, the same subject (role) cannot access the same object for variable number of times. [*Source:* NIST SP 800-192]

"Service Level Agreement (SLA)": Represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination. [*Source:* NIST SP 800-47 Rev. 1]

"Single-Factor Authentication": A characteristic of an authentication system or an authenticator that requires only one authentication factor (something you know, something you have, or something you are) for successful authentication. [*Source:* NIST SP 800-63-3]

"Social Engineering": An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. [*Source:* CNSSI 4009-2015]

"Stakeholder": Individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations. [*Source:* NIST SP 800-160v1r1 from ISO/IEC/IEEE 15288:2015]

"Standard User Account": An account type that is allowed within a system, typically by individuals for regular access to the system. These accounts are defined and managed according to organizational policies and security standards. [*Source:* Aligns with NIST SP 800-53 Rev 5, AC-2, Account Management]

"Subordinate Certificate Authority": In a hierarchical public key infrastructure (PKI), a certificate authority (CA) whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. See superior certification authority. [*Source:* CNSSI 4009-2015]

"Supported Entity": Under Iowa Code section 8.76(13), a "Supported Entity is a unit of state government, which is an authority, board, commission, committee, council, department, or independent agency as defined in Iowa Code section 7E.4, including but not limited to each principal central department enumerated in Iowa Code section 7E.5. However, "Supported Entity" does not include:

a. The office of the governor or the office of an elective constitutional or statutory officer.

b. The general assembly, or any office or unit under its administrative authority.

c. The judicial branch, as provided in Iowa Code section 602.1102.

d. A political subdivision of the state or its offices or units, including but not limited to a county, city, or community college.

e. The state board of regents and institutions operating under its authority.

"System Account": Account type within an information system that allows users to access and manage system resources. System accounts can include various types such as individual, group, temporary, system, guest, anonymous, emergency, developer, and service accounts. Organizations define and manage these accounts to ensure proper access authorizations and to mitigate security risks associated with unauthorized access. [*Source:* NIST SP 800-171 Rev. 3]

"System Maintenance": For the purposes of CyberGUARD information security policies and procedures, system maintenance includes all types of maintenance to any system component (including applications), conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing or information retention such as scanners, copiers, and printers. It does not include application updates performed under release management processes.

"System of Record": An authoritative source for managing and storing change-related documentation and decisions. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. [*Source:* NIST SP 800-53 Rev. 5 from 5 U.S.C., Sec. 552a(a)(5)]

"System Use Notification": A mechanism used to inform individuals about the acceptable use and security policies associated with accessing and interacting with an information system. The purpose of a system use notification is to establish awareness among individuals regarding their responsibilities, the potential monitoring of their activities, and the consequences of unauthorized or improper use of the system. System use notifications can be implemented using messages or warning banners and are displayed before individuals log into the system. [*Source:* Aligns with NIST SP 800-53 Rev 5, AC-8]

"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:* FIPS 200 under ’threat’ from CNSSI 4009- Adapted]

"Unified Endpoint Management (UEM)": Software that enables IT and security teams to monitor, manage, and secure all of an organization’s end-user devices, such as desktops, laptops, tablets, and more, in a consistent manner with a single suite of tools, regardless of operating system or location.

"Unsupported Systems": Includes those for which the manufacturer or vendor no longer provides security updates, patches, or technical support.

"User": Individual or (system) process authorized to access an information system. [*Source:* NIST SP 800-18 Rev 1 under ’user’ from NSSI 4009]

"Vulnerability": Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [*Source:* FIPS 200 under ’vulnerability’ from CNSSI 4009- Adapted]

"Zero-Day Attack": An attack that exploits a previously unknown hardware, firmware, or software vulnerability. [*Source:* CNSSI 4009-2015]