New Hampshire Executive Branch Cybersecurity and Information Security Glossary

8-17-2022

TABLE OF CONTENTS

ACCEPTANCE - AWARENESS 3
BACKDOOR - BUSINESS IMPACT ANALYSIS 16
CALL BACK - CYCLICAL REDUNDANCY CHECK 22
DATA - DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) 39
EAVESDROPPING ATTACK - EXTRANET 45
FAILOVER – FUNCTIONAL TESTING 50
GATEWAY – GROUP AUTHENTICATOR 54
HACKER – HYPERVISOR 54
IDENTIFICATION – IT-RELATED RISK 57
JAILBREAKING – JAVASCRIPT(JS) 70
KERBEROS – KNOWN ERROR 70
LAPTOP COMPUTER – LOW-IMPACT SYSTEM 72
MAINFRAME – MUTUAL AUTHENTICATION 74
NIST – NULL 80
OBJECT – OVERWRITE PROCEDURE 83
PACKET FILTER – PUBLIC KEY INFRASTRUCTURE (PKI) 84
QUALITIY OF SERVICE – RULE-BASED SECURITY TESTING 96
S/MIME – SYSTEM SOFTWARE 103
TABLET – TWO FACTOR AUTHENTICATION 118
UNAUTHORIZED ACCESS – USER ID 122
VALIDATION – VULNERABILITY SCANNING 124
WARM SITE - ZEROIZATION 126

ACCEPTANCE - AWARENESS

Acceptance:
The point at which the end-users of a system declare, formally, that the system meets their needs and has performed satisfactorily during the test procedures. Unless a system has been acquired, installed, or amended, purely for IT department it is not sufficient for technical staff to declare it acceptable; the end users must be involved. (SOURCE: The Information Security Glossary)

Access (Logical):
The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing an ID and password (if required). The view that restricting physical access relieves the need for logical access restrictions is misleading. Any Agency with communications links to the outside world has a security risk of logical access. (SOURCE: The Information Security Glossary)

Access:
Ability to make use of any information system (IS) resource. (SOURCE: NIST SP 800-32)

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

Access Control:
The process of granting or denying specific requests to:

obtain and use information and related information processing services; and

enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances). (SOURCE: FIPS 201; CNSSI-4009)

Access Control List (ACL):
A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity. (SOURCE: CNSSI-4009)

Access Control Mechanism:
Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. (SOURCE: CNSSI-4009)

Access Level:
A category within a given security classification limiting entry or system connectivity to only authorized persons. (SOURCE: CNSSI-4009)

Access List:
Roster of individuals authorized admittance to a controlled area. (SOURCE: CNSSI-4009)

Access Management:
A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data – and only using appropriate and controlled methods. Data Governance programs often focus on supporting Access Management by aligning the requirements and constraints posed by Governance, Risk Management, Compliance, Security, and Privacy efforts. (SOURCE: Data Governance Institute)

Access Point:
A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise network. (SOURCE: NIST SP 800-48; NIST SP 800-121)

Access Profile:
Association of a user with a list of protected objects the user may access. (SOURCE: CNSSI-4009)

Account Management, User:
Involves:
the process of requesting, establishing, issuing, and closing user accounts;
tracking users and their respective access authorizations; and
managing these functions.
(SOURCE: NIST SP 800-12)

Accountability:
The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non- repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (SOURCE: NIST SP 800-27)

Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. (SOURCE: CNSSI-4009)

Activation Data:
Private data, other than keys, that are required to access cryptographic modules.
(SOURCE: NIST SP 800-32)

Active Attack:
An attack that alters a system or data. (SOURCE: CNSSI-4009)

Active Security Testing:
Security testing that involves direct interaction with a target, such as sending packet to a target. (SOURCE: NIST SP 800-115)

Ad Hoc Network:
A wireless network that dynamically connects wireless client devices to each other without the use of an infrastructure device, such as an access point or a base station.
(SOURCE: NIST SP 800-121)

Add-on Security:
Incorporation of new hardware, software, or firmware safeguards in an operational information system. (SOURCE: CNSSI-4009)

Adequate Security:
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. (SOURCE: NIST SP 800-53; FIPS 200; OMB Circular A-130, App. III)

Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Note: This includes assuring that information systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.
(SOURCE: CNSSI-4009; NIST SP 800-37)

Administrative Account:
A user account with full privileges on a computer. (SOURCE: NIST SP 800-69)

Administrative Safeguards:
Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. (SOURCE: NIST SP 800-66)

Advanced Encryption Standard – (AES):
The Advanced Encryption Standard specifies a U.S. government- approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies

the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. (SOURCE: FIPS 197)

A U.S. government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. (SOURCE: CNSSI-4009)

Advanced Key Processor (AKP):
A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to

exchange information with a client platform,

interact with fill devices, and

connect a client platform securely to the primary services node (PRSN).
(SOURCE: CNSSI-4009)

Advanced Persistent Threats (APT):
An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:
pursues its objectives repeatedly over an extended period of time;
adapts to defenders' efforts to resist it; and
is determined to maintain the level of interaction needed to execute its objectives.
(SOURCE: NIST SP 800-39)

Adversary:
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (SOURCE: NIST SP 800-30)

Advisory:
Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. (SOURCE: CNSSI-4009)

Affordable Care Act:
U.S. federal statute signed into law on March 23, 2010, with the goal of expanding public and private insurance coverage and reducing the cost of healthcare for individuals and the government. (SOURCE: IRS PUB 1075)

Agency:
The term “agency” is used to refer to any Department, Agency, Commission, Board, Body, or other instrumentality of the Executive Branch of New Hampshire State Government.

Agent:
A program acting on behalf of a person or organization. (SOURCE: NIST SP 800-95)

Alert:
Notification that a specific attack has been directed at an organization’s information systems. (SOURCE: CNSSI-4009)

Algorithm:
A step-by-step procedure for calculations. Algorithms are used for calculation, data processing, and automated reasoning.

An algorithm is an effective method expressed as a finite list of well-defined instructions for calculating a function. Starting from an initial state and initial input (perhaps empty), the instructions describe a computation that, when executed, proceeds through a finite number of well-defined successive states, eventually producing "output" and terminating at a final ending state. The transition from one state to the next is not necessarily deterministic; some algorithms, known as randomized algorithms, incorporate random input. (SOURCE: WIKIPEDIA)

All-Source Intelligence:
Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence.

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

Analysis:
The examination of acquired data for its significance and probative value to the case. (SOURCE: NIST SP 800-72)

Anomaly-Based Detection:
The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. (SOURCE: NIST SP 800-94)

Anti-spoof:
Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. (SOURCE: CNSSI-4009)

Anti-Virus Software:
A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. (SOURCE: NIST SP 800-83)

Antispyware Software:
A program that specializes in detecting both malware and non- malware forms of spyware. (SOURCE: NIST SP 800-69)

Applicant:
The subscriber is sometimes called an “applicant” after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. (SOURCE: NIST SP 800-32)

Application:
A software program hosted by an information system. (SOURCE: NIST SP 800-37)

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. (SOURCE: CNSSI-4009)

Application Program Interface (API):
An API specifies how some software components should interact with each other. In addition to accessing databases or computer hardware, such as hard disk drives or video cards, an API can be used to ease the work of programming graphical user interface components. In practice, many times an API comes in the form of a library that includes specifications for routines, data structures, object classes, and variables. In some other cases, notably for SOAP and REST services, an API comes as just a specification of remote calls exposed to the API consumers. (SOURCE: WIKIPEDIA)

Application Service Providers (ASPs):
Companies that offer individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers. Sometimes referred to as "apps-on-tap," ASP services are expected to become an important alternative, not only for smaller companies with low budgets for information technology, but also for larger companies as a form of outsourcing and for many services for individuals as well. Most corporations are essentially providing their own ASP service in-house, moving applications off personal computers, and putting them on a special kind of application server that is designed to handle the stripped-down kind of thin-client workstation. This allows an enterprise to reassert the central control over application cost and usage that corporations formerly had prior to the advent of the PC. (SOURCE: TechTarget)

Approval to Operate (ATO):
The official management decision issued by a DAA or PAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (SOURCE: CNSSI-4009)

Approved Mode of Operation:
A mode of the cryptographic module that employs only Approved security functions (not to be confused with a specific mode of an Approved security function, e.g., Data Encryption Standard Cipher- Block Chaining (DES CBC) mode). (SOURCE: FIPS 140-2)

Approved Security Function:
A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either:
specified in an Approved Standard;
adopted in an Approved Standard and specified either in an appendix of the Approved Standard or in a document referenced by the Approved Standard; or
specified in the list of Approved security functions. (SOURCE: FIPS 140-2)

Assessment:
See Security Control Assessment.

Assessment Findings:
Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition. (SOURCE: NIST SP 800-53A)
Assessment Method:
One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment. (SOURCE: NIST SP 800-53A)

Assessment Object:
The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment. (SOURCE: NIST SP 800-53A)

Assessment Procedure:
A set of assessment objectives and an associated set of assessment methods and assessment objects. (SOURCE: NIST SP 800-53A)

Assessor:
See Security Control Assessor.

Asset:
See Information Asset.

Asset Custodian:
A person or group responsible for the day-to-day management, operation, and security of an asset. An asset custodian typically has a role of system, database, or network administrator. Asset custodian is synonymous with data or information custodian.

Asset Identification:
Security Content Automation Protocol (SCAP) constructs to uniquely identify assets (components) based on known identifiers and/or known information about the assets. (SOURCE: NIST SP 800-128)

Asset Owner:
A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, security, and resilience of an organizational asset. For example, the accounts payable department is the owner of the vendor database. (SOURCE: CERT RMM)

Asset Reporting Format (ARF):
SCAP data model for expressing the transport format of information about assets (components) and the relationships between assets and reports. (SOURCE: NIST SP 800-128)

Assurance:
Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes:
functionality that performs correctly,
sufficient protection against unintentional errors (by users or software), and
sufficient resistance to intentional penetration or by-pass.
(SOURCE: NIST SP 800-27)

The grounds for confidence that the set of intended security controls in an information system are effective in their application. (SOURCE: NIST SP 800-37; NIST SP 800-53A)

Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. (SOURCE: CNSSI-4009; NIST SP 800-39)

In the context of OMB M-04-04 and this document, assurance is defined as:
the degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and
the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. (SOURCE: NIST SP 800-63)

Assurance Case:
A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute. (SOURCE: NIST SP 800-53A; NIST SP 800-39)

Assured Information Sharing:
The ability to confidently share information with those who need it, when and where they need it, as determined by operational need and an acceptable level of security risk. (SOURCE: CNSSI-4009)

Assured Software:
Computer application that has been designed, developed, analyzed, and tested using processes, tools, and techniques that establish a level of confidence in it. (SOURCE: CNSSI-4009)

Asymmetric Cryptography:
See Public Key Cryptography. (SOURCE: CNSSI-4009)

Asymmetric Keys:
Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. (SOURCE: FIPS 201)

Asynchronous Transfer Mode (ATM):
A telecommunications concept defined by ANSI and ITU standards for carriage of a complete range of user traffic, including voice, data, and video signals. (SOURCE: WIKIPEDIA)

Attack:
An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. (SOURCE: NIST SP 800-32)

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. (SOURCE: CNSSI-4009)

Attack Sensing and Warning (AS&W):
Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.
(SOURCE: CNSSI-4009)

Attack Signature:
A specific sequence of events indicative of an unauthorized access attempt. (SOURCE: NIST SP 800-12)

A characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities. (SOURCE: CNSSI-4009)

Attack Surface:
The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment.

Attribute-Based Access Control:
Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place. (SOURCE: NIST SP 800-53; CNSSI-4009)

Attribute-Based Authorization:
A structured process that determines when a user is authorized to access information, systems, or services based on attributes of the user and of the information, system, or service. (SOURCE: CNSSI-4009)

Audit:
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. (SOURCE: NIST SP 800-32)
Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. (SOURCE: CNSSI-4009)

Audit Data:
Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. (SOURCE: NIST SP 800-32)

Audit Log:
A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (SOURCE: CNSSI-4009)

Audit Reduction Tools:
Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups. (SOURCE: NIST SP 800-12; CNSSI-4009)

Audit Review:
The assessment of an information system to evaluate the adequacy of implemented security controls, assure that they are functioning properly, identify vulnerabilities, and assist in implementation of new security controls where required. This assessment is conducted annually or whenever significant change has occurred and may lead to recertification of the information system. (SOURCE: CNSSI-4009)

Audit Trail:
A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. (SOURCE: NIST SP 800-47)

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)

Authenticate:
To confirm the identity of an entity when that identity is presented. (SOURCE: NIST SP 800-32)

To verify the identity of a user, user device, or other entity. (SOURCE: CNSSI-4009)

Authentication:
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; FIPS 200; NIST SP 800-30)

The process of establishing confidence of authenticity. (SOURCE: FIPS 201)

Encompasses identity verification, message origin authentication, and message content authentication. (SOURCE: FIPS 190)

A process that establishes the origin of information or determines an entity's identity. (SOURCE: NIST SP 800-21)

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (SOURCE: CNSSI-4009)

The process of establishing confidence in the identity of users or information systems.
(SOURCE: NIST SP 800-63)

Authentication Code:
A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code [MAC]). (SOURCE: FIPS 140-2)

Authentication Mechanism:
Hardware-or software-based mechanisms that force users to prove their identity before accessing data on a device. (SOURCE: NIST SP 800-72; NIST SP 800-124)

Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system. (SOURCE: CNSSI-4009)

Authentication Mode:
A block cipher mode of operation that can provide assurance of the authenticity and, therefore, the integrity of data. (SOURCE: NIST SP 800-38B)

Authentication Period:
The maximum acceptable period between any initial authentication process and subsequent re-authentication processes during a single terminal session or during the period data is being accessed. (SOURCE: CNSSI-4009)

Authentication Protocol:
A defined sequence of messages between a Claimant and a Verifier that demonstrates that the Claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the Claimant that he or she is communicating with the intended Verifier. (SOURCE: NIST SP 800-63)

A well-specified message exchange process between a claimant and a verifier that enables the verifier to confirm the claimant's identity. (SOURCE: CNSSI-4009)

Authentication Tag:
A pair of bit strings associated to data to provide assurance of its authenticity.
(SOURCE: NIST SP 800-38B)

Authentication Token:
Authentication information conveyed during an authentication exchange. (SOURCE: FIPS 196)

Authenticator:
The means used to confirm the identity of a user, process, or device (e.g., user password or token). (SOURCE: NIST SP 800-53; CNSSI-4009)

Authenticity:
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; CNSSI-4009; NIST SP 800-39)

Authority:
Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere. (SOURCE: CNSSI-4009)

Authorization:
Access privileges granted to a user, program, or process or the act of granting those privileges. (SOURCE: CNSSI-4009)

Authorization Boundary:
All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. (SOURCE: CNSSI-4009; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37)

Automated Key Transport:
The transport of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols). (SOURCE: FIPS 140-2)

Automated Security Monitoring:
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)

Autonomous System (AS):
One or more routers under a single administration operating the same routing policy.
(SOURCE: NIST SP 800-54)

Availability:
In the context of information security, refers to ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., Sec. 3542]

Ensuring timely and reliable access to and use of information.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property of being accessible and useable upon demand by an authorized entity.
(SOURCE: CNSSI-4009)

Awareness (Information Security):
Activities which seek to focus an individual's attention on an (information security) issue or set of issues. (SOURCE: NIST SP 800-50)

BACKDOOR - BUSINESS IMPACT ANALYSIS

Backdoor:
Typically, unauthorized hidden software or hardware mechanism used to circumvent security controls. (SOURCE: CNSSI-4009)

An undocumented way of gaining access to a computer system. A backdoor is a potential security risk. (SOURCE: NIST SP 800-82)

Bandwidth:
Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second. (SOURCE: Safety Engineering: Principles and Practices)

Banner:
The information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use. (SOURCE: Intrusion Detection Systems)

Banner Grabbing:
The process of capturing banner information—such as application type and version—that is transmitted by a remote port when a connection is initiated. (SOURCE: NIST SP 800-115)

Baseline:
Hardware, software, databases, and relevant documentation for an information system at a given point in time. (SOURCE: CNSSI-4009)

Baseline Assessment:
An interim compliance validation assessment performed by a QSA to determine the PCI Security compliance status. (SOURCE: VERIZON PCI SECURITY)

Baseline Configuration:
A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. (SOURCE: NIST SP 800-128)

Baseline Security:
The minimum-security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection. (SOURCE: NIST SP 800-16)

Baselining:
Monitoring resources to determine typical utilization patterns so that significant deviations can be detected. (SOURCE: NIST SP 800-61)

Basic Testing:
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing. (SOURCE: NIST SP 800-53A)

Bastion Host:
A special-purpose computer on a network specifically designed and configured to withstand attacks. (SOURCE: CNSSI-4009)

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

Binding:
Process of associating two related elements of information. (SOURCE: NIST SP 800-32)

An acknowledgement by a trusted third party that associates an entity's identity with its public key. This may take place through:
a certification authority's generation of a public key certificate,
a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or
an analogous method.
(SOURCE: NIST SP 800-21)

Process of associating a specific communications terminal with a specific cryptographic key or associating two related elements of information. (SOURCE: CNSSI-4009)

Biometric:
A physical or behavioral characteristic of a human being. (SOURCE: NIST SP 800-32)

A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. (SOURCE: FIPS 201)

Biometric Information:
The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns.) (SOURCE: FIPS 201)

Biometric System:
An automated system capable of 1) capturing a biometric sample from an end user; 2) extracting biometric data from that sample; 3) comparing the extracted biometric data with data contained

in one or more references; 4) deciding how well they match; and 5) indicating whether or not an identification or verification of identity has been achieved.
(SOURCE: FIPS 201)

Biometrics:
Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (SOURCE: CNSSI-4009)

Black Box Testing:
See Basic Testing.

Blacklist:
A list of email senders who have previously sent span to a user. (SOURCE: NIST SP 800-114)

A list of discrete entities, such as hosts or applications that have been previously determined to be associated with malicious activity. (SOURCE: NIST SP 800-94)

Blacklisting:
The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources. (SOURCE: CNSSI-4009)

Blended Attack:
A hostile action to spread malicious code via multiple methods. (SOURCE: CNSSI-4009)

Blinding:
Generating network traffic that is likely to trigger many alerts in a short period of time, to conceal alerts triggered by a "real" attack performed simultaneously. (SOURCE: NIST SP 800-94)

Block:
Sequence of binary bits that comprise the input, output, State, and Round Key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes. (SOURCE: FIPS 197)

Block Cipher:
A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. For a block cipher algorithm, the length of the input block is the same as the length of the output block. (SOURCE: NIST SP 800-90)

Block Cipher Algorithm:

A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length. (SOURCE: NIST SP 800-67)

Blog:
A discussion or informational site published on the World Wide Web and consisting of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first). Blogs may be the work of a single individual, occasionally of a small group, and covering a single subject, or may include posts written by large numbers of authors and professionally edited. (SOURCE: WIKIPEDIA)

Body of Evidence (BoE):
The set of data that documents the information system's adherence to the security controls applied. The BoE will include a Requirements Verification Traceability Matrix (RVTM) delineating where the selected security controls are met and evidence to that fact can be found. The BoE content required by an Authorizing Official will be adjusted according to the impact levels selected. (SOURCE: CNSSI-4009)

Border Gateway Protocol (BGP):
A standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance vector routing protocol. The Border Gateway Protocol does not use Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on paths, network policies and/or rulesets configured by a network administrator. The Border Gateway Protocol plays a key role in the overall operation of the Internet and is involved in making core routing decisions. (SOURCE: WIKIPEDIA)

Boundary Protection:
Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, using boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). (SOURCE: NIST SP 800-53; CNSSI-4009)

Boundary Protection Device:
A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection. (SOURCE: NIST SP 800-53)

A device with appropriate mechanisms that facilitates the adjudication of different security policies for interconnected systems. (SOURCE: CNSSI-4009)

Breach:
The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially

accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose. (SOURCE: US OMB M-17-12)

An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
The unauthorized person who used the protected health information or to whom the disclosure was made;
Whether the protected health information was acquired or viewed; and
The extent to which the risk to the protected health information has been mitigated.
(SOURCE: HIPAA (45 CFR §§ 164.400-414)

Beach of Security:
"Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality, or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure. (SOURCE: N.J.S.A 2C.56:8-161)

Bring Your Own Device (BYOD):
Refers to the policy of permitting employees and contractors to use personally owned or third-party owned mobile devices (e.g., tablets, and smart phones) for State business purposes.
(SOURCE: State of New Hampshire Statewide Information Security Manual)

Brute Force Password Attack:
A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords. (SOURCE: NIST SP 800-72)

Buffer Overflow:
A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. (SOURCE: NIST SP 800-28; CNSSI-4009)

Bulk Encryption:
Simultaneous encryption of all channels of a multichannel telecommunications link.
(SOURCE: CNSSI-4009)

Business Associate:
A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. (SOURCE: US Department of Health and Human Services)

Business Continuity Plan (BCP):
The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. (SOURCE: NIST SP 800-34; CNSSI-4009)

Business Entity:
All trusted Entities that are authorized and/or contracted with a Department and/or Agency within the Executive Branch of State Government for the purpose of this policy Business Entity may include other governmental agencies outside the Executive Branch that do not make use of the Garden State Network. (SOURCE: DOIT Glossary)

Business Impact Analysis (BIA):
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (SOURCE: NIST SP 800-34)

An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. (SOURCE: CNSSI-4009)

CALL BACK - CYCLICAL REDUNDANCY CHECK

Call Back:
Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact. (SOURCE: CNSSI-4009)

Card Skimmer:
A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card. (SOURCE: PCI DSS GLOSSARY)

Card Verification Value (CVV/CVV2):
Both terms are commonly used to refer to the number printed on a card to help secure "card not present" transactions - other terms include CVC, CID and CSC. To be precise, the code printed on the card is the CVV2 - and the CVV is integrity-check data encoded on the magnetic strip - but both terms are widely used online. (SOURCE: VERIZON PCI SECURITY)

Cardholder:
An individual possessing an issued Personal Identity Verification (PIV) card. (SOURCE: FIPS 201)

Cardholder Data Environment (CDE):
All people, processes and technologies that store, process or transmit cardholder data (CHD) or sensitive authentication data (SAD). (SOURCE: VERIZON PCI SECURITY)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD):
A media access control method used most notably in local area networking. It uses a carrier sensing scheme in which a transmitting data station detects other signals while transmitting a frame, and stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame. (SOURCE: WIKIPEDIA)

Category:
Restrictive label applied to classified or unclassified information to limit access. (SOURCE: CNSSI-4009)

Center for Internet Security (CIS) Benchmarks:
CIS benchmarks are configuration baselines and best practices for securely configuring a system**.**

Central Management:
The organization-wide management and implementation of selected security and privacy controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security and privacy controls and processes. (SOURCE: NIST 800-53r5)

Certificate:
A digital representation of information which at least identifies the certification authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it. (SOURCE: NIST SP 800-32)

A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its crypto period. (SOURCE: NIST SP 800-21)

A set of data that uniquely identifies a key pair 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 186)

Certificate Management:
Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (SOURCE: CNSSI-4009)

Certificate Management Authority – (CMA):
A Certification Authority (CA) or a Registration Authority (RA). (SOURCE: NIST SP 800-32)

Certificate of Authority:
In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 standard. (SOURCE: Wikipedia)

Certificate Policy (CP):
A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. (SOURCE: CNSSI-4009; NIST SP 800-32)

Certificate Revocation List (CRL):
A list of revoked public key certificates created and digitally signed by a Certification Authority. (SOURCE: NIST SP 800-63; FIPS 201)

Certification:
A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (SOURCE: FIPS 200)

The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness. (SOURCE: FIPS 201)

Comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. See Security Control Assessment. (SOURCE: CNSSI-4009)

Certification Authority (CA):
A trusted entity that issues and revokes public key certificates. (SOURCE: FIPS 201)

The entity in a public key infrastructure (PKI) that is responsible for issuing certificates and exacting compliance to a PKI policy. (SOURCE: NIST SP 800-21; FIPS 186)

Certification Authority Facility:
The collection of equipment, personnel, procedures, and structures that are used by a Certification Authority to perform certificate issuance and revocation. (SOURCE: NIST SP 800-32)

Certification Package:
Product of the certification effort documenting the detailed results of the certification activities. (SOURCE: CNSSI-4009)

Chain of Custody:
A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. (SOURCE: NIST SP 800-72; CNSSI-4009)

Chain of Evidence:
A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner. (SOURCE: CNSSI-4009)

Change:
The addition, modification, or removal of anything that could influence IT services. The scope should include changes to all architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items. (SOURCE: ITIL V3)

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

Change Control Board (CCB):
A committee that makes decisions regarding whether proposed changes to a software project should be implemented. In short, any changes to the Baseline Requirements agreed with the client, should be taken up by project team on approval from this committee. If any change is agreed by the committee, it is communicated to the project team and client and the requirement is Baselined with the change. The change control board is constituted of project stakeholders or their representatives. The authority of the change control board may vary from project to project, but decisions reached by the change control board are often accepted as final and binding. The decision of acceptance of the changes also depends upon the stage or phase of the project. The main objective is to ensure acceptance of the project (deliverable) by the client.
(SOURCE: WIKIPEDIA)

Check Word:
Cipher text generated by cryptographic logic to detect failures in cryptography. (SOURCE: CNSSI-4009)

Checksum:
Value computed on data to detect error or manipulation. (SOURCE: CNSSI-4009)

Cipher:
Series of transformations that converts plaintext to ciphertext using the Cipher Key. (SOURCE: FIPS 197)

Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both. (SOURCE: CNSSI-4009)

Cipher Block Chaining-Message Authentication Code – (CBC-MAC):
A secret-key block-cipher algorithm used to encrypt data and to generate a Message Authentication Code (MAC) to provide assurance that the payload and the associated data are authentic. (SOURCE: NIST SP 800-38C)

Cipher Suite:
Negotiated algorithm identifiers. Cipher suites are identified in human-readable form using a pneumonic code. (SOURCE: NIST SP 800-52)

Cipher Text Auto-Key (CTAK):
Cryptographic logic that uses previous cipher text to generate a key stream. (SOURCE: CNSSI-4009)

Ciphertext:
Data output from the Cipher or input to the Inverse Cipher. (SOURCE: FIPS 197)

Data in its enciphered form. (SOURCE: NIST SP 800-56B)

Claimant:
A party whose identity is to be verified using an authentication protocol.
(SOURCE: NIST SP 800-63; FIPS 201)

An entity that is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange. (e.g., a smartcard [claimant] can act on behalf of a human user [principal]). (SOURCE: FIPS 196)

An entity (user, device or process) whose assertion is to be verified using an authentication protocol. (SOURCE: CNSSI-4009)

Clear:
To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. See comments on Clear/Purge Convergence. (SOURCE: NIST SP 800-88)

Clear Text:
Information that is not encrypted. (SOURCE: NIST SP 800-82)

Clearing:
Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities (i.e., through the keyboard); however, the data may be reconstructed using laboratory methods. (SOURCE: CNSSI-4009)

Client:
A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server. (SOURCE: NIST SP 800-32)

Closed Security Environment:
Environment providing sufficient assurance that applications and equipment are protected against the introduction of malicious logic during an information system life cycle. Closed security

is based upon a system's developers, operators, and maintenance personnel having sufficient clearances, authorization, and configuration control. (SOURCE: CNSSI-4009)

Cloud Access Security Broker (CASB):
On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention. (SOURCE: Gartner)

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

Note: Both the user's data and essential security services may reside in and be managed within the network cloud. (SOURCE: CNSSI-4009)

CloudConnect:
A bundled offering of cloud-based Microsoft Office365 products, including email, instant messaging, video conferencing, file sharing, and storage. It enables user-friendly interagency communication and file sharing, multi-device content synchronization, and two-factor authenticated remote access. (SOURCE: State of New Hampshire Statewide Information Security Manual)

Cloud Service Provider:
An entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, such as DOIT, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others. (SOURCE: State of New Hampshire Statewide Information Security Manual)

Cold Site:
Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the

building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services. (SOURCE: CNSSI-4009)

A backup facility that has the necessary electrical and physical components of a computer facility but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment if the user must move from their main computing location to an alternate site. (SOURCE: NIST SP 800-34)

Cold Start:
Procedure for initially keying crypto-equipment. (SOURCE: CNSSI-4009)

Collision:
Two or more distinct inputs produce the same output. Also see Hash Function.
(SOURCE: NIST SP 800-57 Part 1)

Comingling:
The presence of FTI and non-FTI data together on the same paper or electronic media.
(SOURCE: IRS PUB 1075)

Common Configuration Enumeration (CCE):
A SCAP specification that provides unique, common identifiers for configuration settings found in a wide variety of hardware and software products. (SOURCE: NIST SP 800-128)

Common Configuration Scoring System (CCSS):
A set of measures of the severity of software security configuration issues. (SOURCE: NISTIR 7502)

A SCAP specification for measuring the severity of software security configuration issues.
(SOURCE: NIST SP 800-128)

Common Platform Enumeration (CPE):
A SCAP specification that provides a standard naming convention for operating systems, hardware, and applications for the purpose of providing consistent, easily parsed names that can be shared by multiple parties and solutions to refer to the same specific platform type. (SOURCE: NIST SP 800-128)

Common Vulnerabilities and Exposures (CVE):
A dictionary of common names for publicly known information system vulnerabilities.
(SOURCE: NIST SP 800-51; CNSSI-4009)

An SCAP specification that provides unique, common names for publicly known information system vulnerabilities. (SOURCE: NIST SP 800-128)

Common Vulnerability Scoring System (CVSS):

An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity. (SOURCE: NIST SP 800-128)

Communications Security (COMSEC):
A component of Information Assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material. (SOURCE: CNSSI-4009)

Comparison:
The process of comparing a biometric with a previously stored reference. (SOURCE: FIPS 201)

Compensating Security Control:
A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.
(SOURCE: CNSSI-4009)

Compliance:
A discipline, set of practices, and/or organizational group that deals with adhering to laws, regulations, standards, and contractual arrangements. Also, the adherence to requirements. Data Governance programs often support many types of compliance requirements: Regulatory compliance, contractual compliance, adherence to internal standards, policies, and architectures, and conformance to rules for data management, project management, and other disciplines. (SOURCE: Data Governance Institute)

Comprehensive Testing:
A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.
(SOURCE: NIST SP 800-53A)

Compromise:
Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. (SOURCE: NIST SP 800-32; CNSSI-4009)

The unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs). (SOURCE: FIPS 140-2)

Component:
A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include

commercial information technology products. Also referred to as a system component. (SOURCE: NIST SP 800-53r4)

Computer-Based Training:
Computer-based training (CBT) is any course of instruction whose primary means of delivery is a computer. A CBT course (sometimes called courseware) may be delivered via a software product installed on a single computer, through a corporate or educational intranet, or over the Internet as Web-based training (SOURCE: TechTarget)

Computer Cryptography:
Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information. (SOURCE: CNSSI-4009)

Computer Emergency Response Team (CERT):
Acronym for Carnegie Mellon University's "Computer Emergency Response Team." The CERT Program develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of critical services. (SOURCE: PCI DSS Glossary)

Computer Incident Response Team (CIRT):
Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team). (SOURCE: CNSSI-4009)

Computer Network Attack (CNA):
Actions taken using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (SOURCE: CNSSI-4009)

Computer Network Defense (CND):
Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (SOURCE: CNSSI-4009)

Computer Network Exploitation (CNE):
Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks. (SOURCE: CNSSI-4009)

Computer Security (COMPUSEC):

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. (SOURCE: CNSSI-4009)

Computer Security Incident:
See incident.

Computer Security Incident Response Team (CSIRT):
A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). (SOURCE: NIST SP 800-61)

Computer Security Object (CSO):
A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. (SOURCE: FIPS 188; CNSSI-4009)

Computer Security Objects Register:
A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects. (SOURCE: FIPS 188; CNSSI-4009)

Computer Security Objects Register:
A collection of Computer Security Object names and definitions kept by a registration authority. (SOURCE: FIPS 188; CNSSI-4009)

Confidentiality:
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542)

The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. (SOURCE: FIPS 140-2)

The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. (SOURCE: CNSSI-4009)

Configuration Control:
Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation. (SOURCE: CNSSI-4009; NIST SP 800-37; NIST SP 800-53)

Configuration Item:
Any component or other service asset that needs to be managed in order to deliver an IT service. (SOURCE: ITIL V3)

Configuration Management:
A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.
(SOURCE: IRS PUB 1075)

Container:
The file used by a virtual disk encryption technology to encompass and protect other files.
(SOURCE: NIST SP 800-111)

Contamination:
Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category. (SOURCE: CNSSI-4009)

Content Filtering:
The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. (SOURCE: NIST SP 800-114)

Contingency Plan:
Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions. (SOURCE: CNSSI-4009)

Continuity of Operations (COOP) Plan:
A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of an disaster event before returning to normal operations. (SOURCE: NIST SP 800-34)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the

capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan. (SOURCE: CNSSI-4009)

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

- The development of a strategy to regularly evaluate selected IA controls/metrics,
- Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events,
- Recording changes to IA controls, or changes that affect IA risks, and
- Publishing the current security status to enable information-sharing decisions involving the enterprise.

(SOURCE: CNSSI-4009)

Maintaining ongoing awareness to support organizational risk decisions. (SOURCE: NIST SP 800-137)

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

Control Information:
Information that is entered into a cryptographic module for the purposes of directing the operation of the module. (SOURCE: FIPS 140-2)

Controlled Access Area:
Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance. (SOURCE: CNSSI-4009)

Controlled Area:
Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. (SOURCE: NIST SP 800-53)

Controlled Interface:
A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems. (SOURCE: CNSSI-4009; NIST SP 800-37)

Cookie:
A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. (SOURCE: NIST SP 800-28)

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. (SOURCE: CNSSI-4009)

Corrective Action Plan (CAP):
A report required to be filed semi-annually, detailing the agency's planned and completed actions to resolve findings identified during an IRS safeguard review. (SOURCE: IRS PUB 1075)

Countermeasures:
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
(SOURCE: NIST SP 800-53; NIST SP 800-37; FIPS 200)

Covert Testing:
Testing performed using covert methods and without the knowledge of the organization's IT staff, but with the full knowledge and permission of upper management. (SOURCE: NIST SP 800-115)

Credential:
An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. (SOURCE: NIST SP 800-63)

Evidence attesting to right to credit or authority. (SOURCE: FIPS 201)

Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once. (SOURCE: CNSSI-4009)

Criminal Justice Information (CJI):
Criminal Justice Information is the term used to refer to all of the FBI Criminal Justice Information Services provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to: biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

Biometric Data - data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, it can include fingerprints, palm prints, iris scans, and facial recognition data.

Identity History Data - textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

Biographic Data - information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

Property Data - information about vehicles and property associated with a crime when accompanied by any personally identifiable information (PII).

Case/Incident History - information about the history of criminal incidents.

(SOURCE: FBI)

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

Critical Infrastructure:
System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)] (SOURCE: CNSSI-4009)

Criticality:
A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. (SOURCE: NIST SP 800-60)

Cross-Site Scripting (XSS):
Vulnerability that is created from insecure coding techniques, resulting in improper input validation. Often used in conjunction with CSRF and/or SQL injection. (SOURCE: PCI DSS Glossary)

Cryptographic Algorithm:
A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (SOURCE: NIST SP 800-21; CNSSI-4009)

Cryptographic Hash Function:
A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:
(One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and
(Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.
(SOURCE: NIST SP 800-21)

Cryptographic Key:
A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: NIST SP 800-63)

A binary string used as a secret parameter by a cryptographic algorithm. (SOURCE: NIST SP 800-108)

A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. (SOURCE: FIPS 201; FIPS 198)
A parameter used in conjunction with a cryptographic algorithm that determines
The transformation of plaintext data into ciphertext data,
The transformation of ciphertext data into plaintext data,
A digital signature computed from data,
The verification of a digital signature computed from data,
An authentication code computed from data, or
An exchange agreement of a shared secret.
(SOURCE: FIPS 140-2)

Cryptographic Token:
A token where the secret is a cryptographic key. (SOURCE: NIST SP 800-63)

A portable, user-controlled physical device (e.g., smart card or PCMCIA card) used to store cryptographic information and possibly also perform cryptographic functions. (SOURCE: CNSSI-4009)

Cryptography:
The discipline that embodies the principles, means, and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. (SOURCE: NIST SP 800-59)

The discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. (SOURCE: NIST SP 800-21)

Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography that makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret. (SOURCE: FIPS 191)

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (SOURCE: CNSSI-4009)

Cryptology:
The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. (SOURCE: NIST SP 800-60)

The mathematical science that deals with cryptanalysis and cryptography. (SOURCE: CNSSI-4009)

Cyber Attack:
An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (SOURCE: CNSSI-4009)

Cyber Incident:
Actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident.
(SOURCE: CNSSI-4009)

Cyber Infrastructure:
Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.
(SOURCE: NISTIR 7628)

Cybersecurity:
The ability to protect or defend the use of cyberspace from cyberattacks. (SOURCE: CNSSI-4009)

The process of protecting information by preventing, detecting, and responding to attacks.
(SOURCE: NIST CYBERSECURITY FRAMEWORK)

Cybersecurity Event:
A change that may have an impact on organizational operations (including mission, capabilities, or reputation). (SOURCE: NIST CYPERSECURITY FRAMEWORK)

Cyberspace:
A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (SOURCE: CNSSI-4009)

Cyclical Redundancy Check (CRC):
A method to ensure data has not been altered after being sent through a communication channel. (SOURCE: NIST SP 800-72)

Error checking mechanism that verifies data integrity by computing a polynomial algorithm-based checksum. (SOURCE: CNSSI-4009)

DATA - DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Data:
A subset of information in an electronic format that allows it to be retrieved or transmitted. (SOURCE: CNSSI-4009)

Data Asset:
Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or Web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a Web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset.
An information-based resource.
(SOURCE: CNSSI-4009)

Data Custodian:
Anyone with physical or operational control of a data repository, including, without limitation, roles such as database administrators, system or server administrators, backup operators and storage server administrators. (SOURCE: Data Governance Institute)

Data Encryption Standard (DES):
The DEA cryptographic engine that is used by the Triple Data Encryption Algorithm (TDEA). (SOURCE: NIST SP 800-67)

Data Governance:
The exercise of authority, control, and shared decision-making (planning, monitoring and enforcement) over the management of data assets. (SOURCE: DAMA DMBOK)

A system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models, which describe who can take what actions with what information, and when, under what circumstances, using what methods. (SOURCE: Data Governance Institute)

Data Integrity:
The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner. (SOURCE: CNSSI-4009)

Data Loss:
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. (SOURCE: NIST SP 800-137)

Data Loss Prevention (DLP):
A system that restricts the transmission of sensitive data, reducing the risk of suffering a breach. (SOURCE: VERIZON PCI SECURITY)

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

Data Security:
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (SOURCE: CNSSI-4009)

Decertification:
Revocation of the certification of an information system item or equipment for cause.
(SOURCE: CNSSI-4009)

Decipher:
Convert enciphered text to plain text by means of a cryptographic system. (SOURCE: CNSSI-4009)

Decode:
Convert encoded text to plain text by means of a code. (SOURCE: CNSSI-4009)

Decrypt:
Generic term encompassing decode and decipher. (SOURCE: CNSSI-4009)

Decryption:
The process of transforming ciphertext into plaintext. (SOURCE: NIST SP 800-67)

The process of changing ciphertext into plaintext using a cryptographic algorithm and key.
(SOURCE: NIST SP 800-21)

Conversion of ciphertext to plaintext using a cryptographic algorithm. (SOURCE: FIPS 185)

Dedicated Mode:
Information systems security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all the following:
valid security clearance for all information within the system,
formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments, and/or special access programs), and
valid need- to-know for all information contained within the information system. When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for

the processing of one type or classification of information, either for full-time operation or for a specified period of time. (SOURCE: CNSSI-4009)

Default Classification:
Classification reflecting the highest classification being processed in an information system. Default classification is included in the caution statement affixed to an object. (SOURCE: CNSSI-4009)

Defense-in-Breadth:
A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). (SOURCE: CNSSI-4009)

Defense-in-Depth:
Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
(SOURCE: CNSSI-4009; NIST SP 800-53)

Degauss:
Procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. (SOURCE: CNSSI-4009)

Deleted File:
A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data. (SOURCE: NIST SP 800-72)

Demilitarized Zone (DMZ):
An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. (SOURCE: NIST SP 800-41)

A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. (SOURCE: NIST SP 800-45)

Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted (SOURCEs with restricted access to releasable information while shielding the internal networks from outside attacks. (SOURCE: CNSSI-4009)

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: CNSSI-4009)

Deny by Default / Allow by Exception:
A firewall configuration policy that forces the user to register at the site, authenticate and authorize prior to gaining access. (SOURCE: SECUROSIS WEBSITE)

Depth:
An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive. (SOURCE: NIST SP 800-53A)

Digital Evidence:
Electronic information stored or transferred in digital form. (SOURCE: NIST SP 800-72)

Digital Forensics:
The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. (SOURCE: NIST SP 800-86)

Digital Signature:
An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation. (SOURCE: NIST SP 800-63)

A non-forgeable transformation of data that allows the proof of the (SOURCE (with non-repudiation) and the verification of the integrity of that data. (SOURCE: FIPS 196)

The result of a cryptographic transformation of data which, when properly implemented, provides the services of:
origin authentication,
data integrity, and
signer non-repudiation.
(SOURCE: FIPS 140-2)

The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity, and signatory non-repudiation. (SOURCE: FIPS 186-3)

The result of a cryptographic transformation of data that, when properly implemented, provides origin authentication, data integrity, and signatory non-repudiation. (SOURCE: NIST SP 800-89)

Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay. (SOURCE: CNSSI-4009)

Digital Signing:
An attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users' private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the 'digitally signed' document) that can only be decrypted by applying the user's public key. (Also digitally signing, digital signature)

Direct-Attached Storage (DAS):
A digital storage system directly attached to a server or workstation, without a storage network in between. (SOURCE: WIKIPEDIA)

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)

Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days.

See Continuity of Operations Plan and Contingency Plan. (SOURCE: CNSSI-4009)

Discretionary Access Control:
The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control. (SOURCE: FIPS 191)

A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). (SOURCE: CNSSI-4009)

Disruption:
An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (SOURCE: CNSSI-4009)

An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). (SOURCE: NIST SP 800-34)

Distributed Denial of Service – (DDoS):
A Denial-of-Service technique that uses numerous hosts to perform the attack. (SOURCE: CNSSI-4009)

Domain:
A set of subjects, their information objects, and a common security policy. (SOURCE: NIST SP 800-27)

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See Security Domain. (SOURCE: CNSSI-4009; NIST SP 800-53; NIST SP 800-37)

Domain Name System (DNS):
A hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet, that has been in use since 1985. (SOURCE: Wikipedia)

Dynamic Host Configuration Protocol (DHCP):
A standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually. (SOURCE: WIKIPEDIA)

EAVESDROPPING ATTACK - EXTRANET

Eavesdropping Attack:
An attack in which an Attacker listens passively to the authentication protocol to capture information that can be used in a subsequent active attack to masquerade as the Claimant. (SOURCE: NIST SP 800-63)

Egress Filtering:
Filtering of outgoing network traffic. (SOURCE: NIST SP 800-41)

Electronic Authentication (E-authentication):
The process of establishing confidence in user identities electronically presented to an information system. (SOURCE: NIST SP 800-63; CNSSI-4009)

Electronic Key Entry:
The entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator of the key may have no knowledge of the value of the key being entered.) (SOURCE: FIPS 140-2)

Electronic Key Management System (EKMS):
Interoperable collection of systems being developed by services and agencies of the U.S. government to automate the planning, ordering, generating, distributing, storing, filling, using, and destroying of electronic key and management of other types of COMSEC material. (SOURCE: CNSSI-4009)

Electronic Messaging Services:
Services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business. (SOURCE: CNSSI-4009)

Electronic Signature:
The process of applying any mark in electronic form with the intent to sign a data object. See also Digital Signature. (SOURCE: CNSSI-4009)

Embedded Cryptographic System:
Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem. (SOURCE: CNSSI-4009)

Embedded Cryptography:
Cryptography engineered into an equipment or system whose basic function is not cryptographic. (SOURCE: CNSSI-4009)

Embedded System:
An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Some examples of embedded systems include ATMs, cell phones, printers, thermostats, calculators, and videogame consoles. (SOURCE: Wikipedia)

Embedded Technology:
Specialized hardware and software that is wholly incorporated as part of a larger system or machine. (SOURCE: Army Knowledge Management and Information Technology)

Encode:
Convert plain text to cipher text by means of a code. (SOURCE: CNSSI-4009)

Encrypt:
Generic term encompassing encipher and encode. (SOURCE: CNSSI-4009)

Encrypted Key:
A cryptographic key that has been encrypted using an approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key. (SOURCE: FIPS 140-2)

Encrypted Network:
A network on which messages are encrypted (e.g., using DES, AES, or other appropriate algorithms) to prevent reading by unauthorized parties. (SOURCE: NIST SP 800-32)

Encryption:
Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. (SOURCE: FIPS 185)

The process of changing plaintext into ciphertext for the purpose of security or privacy.
(SOURCE: NIST SP 800-21; CNSSI-4009)

Encryption Algorithm:
Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. (SOURCE: CNSSI-4009)

Encryption Certificate:
A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
(SOURCE: NIST SP 800-32)

End-to-End Encryption:

Communications encryption in which data is encrypted when being passed through a network, but routing information remains visible. (SOURCE: NIST SP 800-12)

Encryption of information at its origin and decryption at its intended destination without intermediate decryption. (SOURCE: CNSSI-4009)

End-to-End Security:
Safeguarding information in an information system from point of origin to point of destination. (SOURCE: CNSSI-4009)

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

Enterprise:
An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. (SOURCE: CNSSI-4009)

Enterprise Architecture (EA):
The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. (SOURCE: CNSSI-4009)

Enterprise Risk Management:
The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.
(SOURCE: CNSSI-40)

Entity:
Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information). (SOURCE: NIST SP 800-27)

An active element in an open system. (SOURCE: FIPS 188)

Any participant in an authentication exchange; such a participant may be human or nonhuman and may take the role of a claimant and/or verifier. (SOURCE: FIPS 196)

Entrapment:
Deliberate planting of apparent flaws in an IS for the purpose of detecting attempted penetrations. (SOURCE: CNSSI-4009)

Entropy:
A measure of the amount of uncertainty that an Attacker faces to determine the value of a secret. Entropy is usually stated in bits. (SOURCE: NIST SP 800-63)

Environment:
Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. (SOURCE: FIPS 200; CNSSI-4009)

Erasure:
Process intended to render magnetically stored information irretrievable by normal means. (SOURCE: CNSSI-4009)

Error Detection Code:
A code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data. (SOURCE: FIPS 140-2; CNSSI-4009)

Escrow:
Something (e.g., a document, an encryption key) that is "delivered to a third person to be given to the grantee only upon the fulfillment of a condition." (SOURCE: FIPS 185)

Event:
Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. (SOURCE: CNSSI-4009; NIST SP 800-61)

Examination:
A technical review that makes the evidence visible and suitable for analysis; tests performed on the evidence to determine the presence or absence of specific data. (SOURCE: NIST SP 800-72)

Examine:
A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time. (SOURCE: NIST SP 800-53A)

Exculpatory Evidence:
Evidence that tends to decrease the likelihood of fault or guilt. (SOURCE: NIST SP 800-72)

Expected Output:
Any data collected from monitoring and assessments as part of the Information Security Continuous Monitoring (ISCM) strategy. (SOURCE: NIST SP 800-137)

Exploit Code:
A program that allows attackers to automatically break into a system. (SOURCE: NIST SP 800-40)

External Information System (or Component):
An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-40)

External Information System Service Provider:
A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (SOURCE: NIST SP 800-37; NIST SP 800-53)

External Network:
A network not controlled by the organization. (SOURCE: NIST SP 800-53; CNSSI-4009)

External Party:
A person external to New Hampshire State Government.

External Security Testing:
Security testing conducted from outside the organization's security perimeter.
(SOURCE: NIST SP 800-115)

Extranet:
A private network that uses Web technology, permitting the sharing of portions of an enterprise's information or operations with suppliers, vendors, partners, customers, or other enterprises. (SOURCE: CNSSI-4009)

FAILOVER – FUNCTIONAL TESTING

Failover:
The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. (SOURCE: NIST SP 800-53; CNSSI-4009)

Failure Access:
Type of incident in which unauthorized access to data results from hardware or software failure. (SOURCE: CNSSI-4009)

Failure Control:
Methodology used to detect imminent hardware or software failure and provide fail safe or fail-soft recovery. (SOURCE: CNSSI-4009)

False Acceptance:
When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity. (SOURCE: NIST SP 800-76)

In biometrics, the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out. (SOURCE: CNSSI-4009)

The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. (SOURCE: NIST SP 800-76)

The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.
(SOURCE: CNSSI-4009)

False Positive:
An alert that incorrectly indicates that malicious activity is occurring. (SOURCE: NIST SP 800-61)

Federal Identity, Credentials, and Access Management (FICAM):
The programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and NPEs, bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources. ICAM cuts across numerous offices, programs, and systems within an agency's enterprise, which are typically directed and managed separately. As

a result, many of the aspects of ICAM within the Federal Government have traditionally been managed within individual stovepipes. The following figure provides a high-level overview of the complementary nature of different parts of ICAM and how concepts that were once viewed as stovepipes can intersect to provide an enterprise capability. (SOURCE: FICAM ROADMAP AND IMPLEMENTATION GUIDANCE)

Federal Information Processing Standard (FIPS):
A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability. (SOURCE: FIPS 201)

Federal Information Security Management Act (FISMA):
A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB. (SOURCE: CNSSI-4009)

Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided. (SOURCE: NIST SP 800-63)

Federal Risk and Authorization Management Program (FedRAMP):
A federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
(SOURCE: http://cloud.cio.gov/fedramp)

Federal Tax Information (FTI) – Federal Tax information consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(b) agreement. FTI includes any information created by the recipient that is derived from Federal return or return information received from the IRS or obtained through a secondary source. (SOURCE: IRS).

File Encryption:
The process of encrypting individual files on a storage medium and permitting access to the encrypted data only after proper authentication is provided. (SOURCE: NIST SP 800-111)

File Protection:
Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents. (SOURCE: CNSSI-4009)

File Security:
Means by which access to computer files is limited to authorized users only. (SOURCE: CNSSI-4009)

File Transfer Protocol (FTP):
Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology. (SOURCE: PCI DSS GLOSSARY)

Firewall:
A gateway that limits access between networks in accordance with local security policy.
(SOURCE: NIST SP 800-32)

A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. (SOURCE: CNSSI-4009)

A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. (SOURCE: NIST SP 800-41)

Firewall Control Proxy:
The component that controls a firewall's handling of a call. The firewall control proxy can instruct the firewall to open specific ports that are needed by a call and direct the firewall to close these ports at call termination. (SOURCE: NIST SP 800-58)

Firmware:
The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution. (SOURCE: FIPS 140-2)

Computer programs and data stored in hardware - typically in read- only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. (SOURCE: CNSSI-4009)

Flash:
A multimedia and software platform used for creating vector graphics, animation, games, and rich Internet applications (RIAs) that can be viewed, played and executed in Adobe Flash Player. Flash is frequently used to add streamed video or audio players, advertisement, and interactive multimedia content to web pages. (SOURCE: WIKIPEDIA)

Flaw:
Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. (SOURCE: CNSSI-4009)

Flooding:
An attack that attempts to cause a failure in a system by providing more input than the system can process properly. (SOURCE: CNSSI-4009)

Forensics:
The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (SOURCE: CNSSI-4009)

Frame Relay:
A standardized wide area network (WAN) technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces. (SOURCE: WIKIPEDIA)

Full Disk Encryption (FDE):
The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. (SOURCE: NIST SP 800-111)

Function:
A team or group of people and the tools or other resources they use to carry out one or more processes or activities. (SOURCE: ITIL V3)

Functional Testing:
Segment of security testing in which advertised security mechanisms of an information system are tested under operational conditions. (SOURCE: CNSSI-4009)

GATEWAY – GROUP AUTHENTICATOR

Gateway:
Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. (SOURCE: CNSSI-4009)

Gateways:
Points (network point, device, software, etc.) that act as an entrance to another point (network, computer, software application, etc.).

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

Governance, Risk, and Compliance (GRC):
Governance, Risk, and Compliance is a term often used by management to acknowledge the interdependencies of these three disciplines in setting policy. See also GRC-SQ and Risk Management. (SOURCE: Data Governance Institute)

Group Authenticator:
Used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group. (SOURCE: CNSSI-4009)

HACKER – HYPERVISOR

Hacker:
Unauthorized user who attempts to or gains access to an information system.
(SOURCE: CNSSI-4009)

Handshaking Procedures:
Dialogue between two information systems for synchronizing, identifying, and authenticating themselves to one another. (SOURCE: CNSSI-4009)

Hash Value:
The result of applying a cryptographic hash function to data (e.g., a message).
(SOURCE: NIST SP 800-106)

Hashing:
The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data. (SOURCE: NIST SP 800-72; CNSSI-4009)

Health information:
means any information, whether oral or recorded in any form or medium, that:

> is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
>
> relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(SOURCE: HIPAA)

High Availability:
A failover feature to ensure availability during device or component interruptions.
(SOURCE: NIST SP 800-113)

High Impact:
The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e.,
causes a severe degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced; results in major damage to organizational assets; results in major financial loss; or
results in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries). (SOURCE: FIPS 199; CNSSI-400)

High-Impact System:
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200)

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high. (SOURCE: CNSSI-4009)

HIPAA:
The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the

Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. (SOURCE: WIKIPEDIA)

HITECH:
The Health Information Technology for Economic and Clinical Health Act, abbreviated HITECH Act, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5). Under the HITECH Act, the United States Department of Health and Human Services is spending $25.9 billion to promote and expand the adoption of health information technology. (SOURCE: WIKIPEDIA)

Honeypot:
A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. (SOURCE: CNSSI-4009)

Host:
A computer dedicated to providing services to many users. Examples of such systems include mainframes, minicomputers, or servers that provide dynamic host configuration protocol services. (SOURCE: IRS PUB 1075)

Hot Site:
A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption. (SOURCE: NIST SP 800-34)

Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization. (SOURCE: CNSSI-4009)

Hybrid Security Control:
A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See also Common Control and System-Specific Security Control. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

Hypertext Transfer Protocol (HTTP):
An application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext. (SOURCE: WIKIPEDIA)

Hypertext Transfer Protocol Over Secure Socket Layer (HTTPS):
Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins. (SOURCE: PCI GLOSSARY)

Hypervisor:
Software or firmware responsible for hosting and managing virtual machines. For the purposes of PCI DSS, the hypervisor system component also includes the virtual machine monitor (VMM). (SOURCE: PCI DSS GLOSSARY)

IDENTIFICATION – IT-RELATED RISK

Identification:
The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (SOURCE: NIST SP 800-47)

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. (SOURCE: FIPS 201)

An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others. (SOURCE: CNSSI-4009)

Identifier:
Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. (SOURCE: FIPS 201)

A data object - often, a printable, non-blank character string - that definitively represents a specific identity of a system entity, distinguishing that identity from all others. (SOURCE: CNSSI-4009)

Identity:
A set of attributes that uniquely describe a person within a given context. (SOURCE: NIST SP 800-63)

The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (SOURCE: FIPS 201)

The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity. (SOURCE: CNSSI-4009)

Identity Proofing:
The process by which a Credentials Service Provider (CSP) and a Registration Authority (RA) collect and verify information about a person for the purpose of issuing credentials to that person. (SOURCE: NIST SP 800-63)

The process of providing sufficient information (e.g., identity history, credentials, documents) to a Personal Identity Verification Registrar when attempting to establish an identity. (SOURCE: FIPS 201)

Identity Registration:
The process of making a person's identity known to the Personal Identity Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system. (SOURCE: FIPS 201; CNSSI-4009)

Identity Token:
Smart card, metal key, or other physical object used to authenticate identity. (SOURCE: CNSSI-4009)

Identity Validation:
Tests enabling an information system to authenticate users or resources. (SOURCE: CNSSI-4009)

Identity Verification:
The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card of system and associated with the identity being claimed. (SOURCE: FIPS 201; NIST SP 800-79)

Identity-Based Access Control:
Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. (SOURCE: NIST SP 800-53; CNSSI-4009)

Identity-Based Security Policy:
A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access.
(SOURCE: NIST SP 800-33)

Individually Identifiable Health Information:
Information that is a subset of health information, including demographic information collected from an individual, and:

> Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

That identifies the individual; or

With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(SOURCE: HIPAA)

Impact:
The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (SOURCE: NIST SP 800-60)

Impact Level:
The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (SOURCE: CNSSI-4009)

High, Moderate, or Low security categories of an information system established in FIPS 199 which classify the intensity of a potential impact that may occur if the information system is jeopardized. (SOURCE: NIST SP 800-34)

Inadvertent Disclosure:
Type of incident involving accidental exposure of information to an individual not authorized access. (SOURCE: CNSSI-4009)

Incident (ITIL):
An unplanned interruption to an IT service, or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident.
(SOURCE: ITIL V3 SERVICE OPERATION 7.2.2)

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (SOURCE: NIST SP 800-61)

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information 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; NIST SP 800-53)

An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information 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: CNSSI-4009)

Incident Handling:
The mitigation of violations of security policies and recommended practices. (SOURCE: NIST SP 800-61)

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-attacks against an organization's information system(s). (SOURCE: NIST SP 800-34)

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT system(s). (SOURCE: CNSSI-4009)

Indicator of Compromise (IOC):
A forensic artifact or remnant of an intrusion that can be identified on a host or network.
(SOURCE: RSA, DIVISION OF EMC)

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

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.
(SOURCE: CNSSI-4009)

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

Information Assurance (IA):
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (SOURCE: NIST SP 800-59; CNSSI-4009)

Information Owner:
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. See Information Steward.
(SOURCE: FIPS 200; NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; NIST SP 800-18; CNSSI-4009)

Information Processing Facilities:
The physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

Information Resources:
Information and related resources, such as personnel, equipment, funds, and information technology. (SOURCE: FIPS 200; FIPS 199; NIST SP 800-53; NIST SP 800-18; NIST SP 800-60; 44 U.S.C., Sec. 3502; CNSSI-4009)

Information Security:
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec.3542)

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide—

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information.

(SOURCE: NIST SP 800-66; 44 U.S.C., Sec 3541)

Information Security Architecture:
An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. (SOURCE: NIST SP 800-39)

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

Information 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. (SOURCE: NIST SP 800-137)

Information Security Policy:
Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
(SOURCE: NIST SP 800-53; NIST SP 800-37; NIST SP 800-18; CNSSI-4009)

Information Security Risk:
The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk. (SOURCE: NIST SP 800-30)

Information System:
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (SOURCE: FIPS 200; FIPS 199; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-18; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (SOURCE: NIST SP 800-53; CNSSI-4009)

Information System Contingency Plan (ISCP):
Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. (SOURCE: NIST SP 800-34)

Information System Owner:
(a.k.a. Program Manager) Individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-60)

Information System Resilience:
The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. (SOURCE: NIST SP 800-30)

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: NIST SP 800-39)

Information System Security Officer (ISSO):
Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-37; NIST SP 800-53)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-53A; NIST SP 800-60)

Information System-Related Security Risks:
Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation). See Risk. (SOURCE: NIST SP 800-37; NIST SP 800-53A)

Information Systems Security Officer (ISSO):
Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (SOURCE: CNSSI-4009)

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. (SOURCE: NIST SP 800-39)

Information System Service:
A capability provided by an information system that facilitates information processing, storage, or transmission. Also referred to as a service.

Information Technology:
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the

equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:
Requires the use of such equipment; or
Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009; 40 U.S.C., Sec. 11101 and Sec 1401)

Information Technology Resources:
Information and communications technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants)

Information Type:
A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009)

Infrastructure as a Service:
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, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (SOURCE: Cloud Security Alliance)

Ingress Filtering:
Method of filtering inbound network traffic such that only explicitly allowed traffic is permitted to enter the network. (SOURCE: PCI DSS GLOSSARY)

Injection Flaws:
Vulnerability that is created from insecure coding techniques resulting in improper input validation, which allows attackers to relay malicious code through a web application to the underlying system. This class of vulnerabilities includes SQL injection, LDAP injection, and XPath injection. (SOURCE: PCI DSS GLOSSARY)

Insecure Protocol/Service/Port:
A protocol, service, or port that introduces security concerns due to the lack of controls over confidentiality and/or integrity. These security concerns include services, protocols, or ports that

transmit data or authentication credentials (for example, password/passphrase) in clear-text over the Internet, or that easily allow for exploitation by default or if misconfigured. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2. (SOURCE: PCI DSS GLOSSARY)

Inside Threat:
An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. (SOURCE: NIST SP 800-32)

Integrity:
Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; NIST SP 800-27; NIST SP 800-37; NIST SP 800-60; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (SOURCE: FIPS 140-2)

The property whereby an entity has not been modified in an unauthorized manner.
(SOURCE: CNSSI-4009)

Integrity Check Value:
Checksum capable of detecting modification of an information system. (SOURCE: CNSSI-4009)

Intellectual Property:
Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. (SOURCE: NIST SP 800-32)

Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered. (SOURCE: CNSSI-4009)

Interconnection Security Agreement (ISA):
An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations. (SOURCE: NIST SP 800-47)

A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical,

procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection. (SOURCE: CNSSI-4009)

Interface:
A shared boundary across which two or more separate components of a computer system exchange information. The exchange can be between software, computer hardware, peripheral devices, humans and combinations of these. (SOURCE: Wikipedia)

Common boundary between independent systems or modules where interactions take place. (SOURCE: CNSSI-4009)

Internal Network:
A network where:
the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or

cryptographic encapsulation or similar security technology provides the same effect.

An internal network is typically organization-owned yet may be organization-controlled while not being organization-owned. (SOURCE: NIST SP 800-53; CNSSI-4009)

Internal Revenue Service (IRS) Publication (Pub) 1075:
This publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Taxpayer Information (FTI). (SOURCE: IRS PUB. 1075)

Internal Security Controls:
Hardware, firmware, or software features within an information system that restrict access to resources only to authorized subjects. (SOURCE: CNSSI-4009)

Internal Security Testing:
Security testing conducted from inside the organization's security perimeter.
(SOURCE: NIST SP 800-115

International Organization for Standardization (ISO):
Non-governmental organization consisting of a network of the national standards institutes.
(SOURCE: PCI DSS GLOSSARY)

Internet:
The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share
the protocol suite specified by the Internet Architecture Board (IAB), and
the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

(SOURCE: CNSSI-4009)

Internet Group Management Protocol (IGMP):
A communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast. IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. (SOURCE: Wikipedia)

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

Internet Message Access Protocol (IMAP):
An application-layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server. (SOURCE: PCI DSS GLOSSARY)

Internet Protocol (IP):
Standard protocol for transmission of data from (SOURCE to destinations in packet-switched communications networks and interconnected systems of such networks. (SOURCE: CNSSI-4009)

Internet Protocol Telephony (IP Telephony):
See Voice over Internet Protocol (VoIP).

Interoperability:
The ability of making systems and organizations to work together (inter-operate). While the term was initially defined for information technology or systems engineering services to allow for information exchange, a broader definition takes into account social, political, and organizational factors that impact system to system performance. (SOURCE: Wikipedia)

Intranet:
A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). (SOURCE: CNSSI-4009)

Intrusion:
Unauthorized act of bypassing the security mechanisms of a system. (SOURCE: CNSSI-4009)

Intrusion Detection Systems (IDS):
Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
(SOURCE: CNSSI-4009)

Intrusion Prevention Systems (IPS):
Network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. (SOURCE: Wikipedia)

IP Security (IPsec):
Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment. (SOURCE: CNSSI-4009)

ISO27000:
A family of standards published by the International Organization for Standardization designed to keep information assets secure. ISO 27001 provides requirements for an information security management system. (SOURCE: ISO WEBSITE)

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

IT Infrastructure Library (ITIL):
A public framework that describes best practice in IT service management. (SOURCE: ITIL V3)

A series of publications providing Best Practice guidance for IT Service Management.
(SOURCE: Data Governance Institute)

IT Portfolio Management:
A key function of IT Governance, IT portfolio management is the formal process for managing IT assets such as software, hardware, middleware, an IT project, internal staff, an application or external consulting. (SOURCE: Data Governance Institute)

IT Security Architecture:
A description of security principles and an overall approach for complying with the principles that drive the system design, i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments. (SOURCE: NIST SP 800-27)

IT Security Awareness:
The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. (SOURCE: NIST SP 800-50)

IT Security Awareness and Training Program:
Explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed.

(SOURCE: NIST SP 800-50; CNSSI-4009)

IT Security Policy:
The "documentation of IT security decisions" in an organization.

NIST SP 800-12 categorizes IT Security Policy into three basic types:
Program Policy—high-level policy used to create an organization's IT security program, define its scope within the organization, assign implementation responsibilities, establish strategic direction, and assign resources for implementation.
Issue-Specific Policies—address specific issues of concern to the organization, such as contingency planning, the use of a particular methodology for systems risk management, and implementation of new regulations or law. These policies are likely to require more frequent revision as changes in technology and related factors take place.
System-Specific Policies—address individual systems, such as establishing an access control list or in training users as to what system actions are permitted. These policies may vary from system to system within the same organization. In addition, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's electronic mail (email) policy or fax security policy.
(SOURCE: NIST SP 800-35)

IT Security Training:
IT Security Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing). The most significant difference between training and awareness is that training seeks to teach skills, which allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or set of issues.

The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. (SOURCE: NIST SP 800-50)

IT Service Management (ITSM):
The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process, and Information Technology. (Baseline IT definition) (SOURCE: Data Governance Institute)

IT-Related Risk:
The net mission/business impact considering
The likelihood that a particular threat (SOURCE will exploit, or trigger, a particular information system vulnerability, and
The resulting impact if this should occur. IT-related risks arise from legal liability or mission/business loss due to, but not limited to:
Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information;

Non-malicious errors and omissions;
IT disruptions due to natural or man-made disasters; or
Failure to exercise due care and diligence in the implementation and operation of IT.
(SOURCE: NIST SP 800-27)

JAILBREAKING – JAVASCRIPT(JS)

Jailbreaking:
Modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator, e.g., to allow the installation of unauthorized software.
(SOURCE: State of New Hampshire Statewide Information Security Manual)

JAVA:
A computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that code that runs on one platform does not need to be recompiled to run on another. Java applications are typically compiled to bytecode (class file) that can run on any Java virtual machine (JVM) regardless of computer architecture. (SOURCE: Wikipedia)

JavaScript (JS):
A dynamic computer programming language most used as part of web browsers, whose implementations allow client-side scripts to interact with the user, control the browser, communicate asynchronously, and alter the document content that is displayed. (SOURCE: Wikipedia)

KERBEROS – KNOWN ERROR

Kerberos:
A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob. When Kerberos authentication is based on passwords, the protocol is known to be vulnerable to off-line dictionary attacks by eavesdroppers who capture the initial user-to- KDC exchange. Longer password length and complexity provide some mitigation to this vulnerability, although sufficiently long passwords tend to be cumbersome for users. (SOURCE: NIST SP 800-63)

A means of verifying the identities of principals on an open network. It accomplishes this without relying on the authentication, trustworthiness, or physical security of hosts while assuming all packets can be read, modified, and inserted at will. It uses a trust broker model and symmetric

cryptography to provide authentication and authorization of users and systems on the network. (SOURCE: NIST SP 800-95)

Key:
A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: NIST SP 800-63)

A numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. (SOURCE: CNSSI-4009)

A parameter used in conjunction with a cryptographic algorithm that determines its operation. Examples applicable to this Standard include:
The computation of a digital signature from data, and
The verification of a digital signature.
(SOURCE: FIPS 186)

Key Exchange:
The process of exchanging public keys in order to establish secure communications.
(SOURCE: NIST SP 800-32; CNSSI-4009)

Key Logger:
A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures. (SOURCE: NIST SP 800-82)

Key Management:
The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. (SOURCE: FIPS 140-2; CNSSI-4009)

Key Management Infrastructure (KMI):
All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users.
(SOURCE: CNSSI-4009)

Key Pair:
Two mathematically related keys having the properties that
one key can be used to encrypt a message that can only be decrypted using the other key, and
even knowing one key, it is computationally infeasible to discover the other key. (SOURCE: NIST SP 800-32)
A public key and its corresponding private key; a key pair is used with a public key algorithm. (SOURCE: NIST SP 800-21; CNSSI-4009)

Known Error:
A problem that has a documented root cause and a workaround. (SOURCE: ITIL V3)

LAPTOP COMPUTER – LOW-IMPACT SYSTEM

Laptop Computer:
A portable computer, small enough to rest on the user's lap and having a screen that closes over the keyboard like a lid. Unlike a mobile device, a laptop computer has a computer operating system, and often more robust data storage and peripheral connection capabilities.
(SOURCE: Modern Technology As Instructional Devices)

Layer Three Switch:
Routers that switch based on Layer 3 information, using ASICs/hardware instead of the CPU/software. Layer three switches differ from layer two switches in that they process data faster using different technology. (SOURCE: Wikipedia)

Layer Two Switch:
Network switch utilizing Layer 2 Tunneling Protocol (L2TP), an IETF standard that can be used as an alternative protocol to Multiprotocol Label Switching (MPLS) for encapsulation of multiprotocol Layer 2 communications traffic over IP networks. L2TP provides a pseudo-wire service. (SOURCE: Wikipedia)

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

Least Privilege:
The security objective of granting users only those accesses they need to perform their official duties. (SOURCE: NIST SP 800-12)

The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (
SOURCE: CNSSI-4009)

Least Trust:
The principal that a security architecture should be designed in a way that minimizes 1) the number of components that require trust, and 2) the extent to which each component is trusted. (SOURCE: CNSSI-4009)

Level of Protection:
Extent to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. Levels of protection are:

- Basic: information systems and networks requiring implementation of standard minimum security countermeasures.
- Medium: information systems and networks requiring layering of additional safeguards above the standard minimum security countermeasures.
- High: information systems and networks requiring the most stringent protection and rigorous security countermeasures.

(SOURCE: CNSSI-4009)

Lightweight Directory Access Protocol (LDAP):
Authentication and authorization data repository utilized for querying and modifying user permissions and granting access to protected internal resources. (SOURCE: PCI DSS GLOSSARY)

Likelihood of Occurrence:
In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability. (SOURCE: CNSSI-4009)

Link Encryption:
Link encryption encrypts all the data along a communications path (e.g., a satellite link, telephone circuit, or T1 line). Since link encryption also encrypts routing data, communications nodes need to decrypt the data to continue routing. (SOURCE: NIST SP 800-12)

Encryption of information between nodes of a communications system. (SOURCE: CNSSI-4009)

List-Oriented:
Information system protection in which each protected object has a list of all subjects authorized to access it. (SOURCE: CNSSI-4009)

Local Access:
Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.
(SOURCE: NIST SP 800-53; CNSSI-4009)

Local Area Network (LAN):
A group of computers and/or other devices that share a common communications line, often in a building or group of buildings. (SOURCE: PCI DSS GLOSSARY)

Local Authority:
Organization responsible for generating and signing user certificates in a PKI-enabled environment. (SOURCE: CNSSI-4009)

Logical Partition (LPAR):
A system of subdividing, or partitioning, a computer's total resources—processors, memory and storage—into smaller units that can run with their own, distinct copy of the operating system and applications. Logical partitioning is typically used to allow the use of different operating systems and applications on a single device. The partitions may or may not be configured to communicate with each other or share some resources of the server, such as network interfaces. (SOURCE: PCI DSS GLOSSARY)

Low Impact:
The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States i.e.
causes a degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced;
results in minor damage to organizational assets; results in minor financial loss; or
results in minor harm to individuals. (SOURCE: CNSSI-4009)

Low-Impact System:
An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-60; FIPS 200; CNSSI-4009)

MAINFRAME – MUTUAL AUTHENTICATION

Mainframe:
Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design. (SOURCE: PCI DSS GLOSSARY)

Major Application:
A major application or system is defined as any system or application that includes one or more of the following characteristics:
Includes users in more than one agency;
Costs more than $200,000 to develop and implement (cost includes hardware, software, and contract personnel);
Any public facing web application; and/or
Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.
(SOURCE: State of New Hampshire Statewide Information Security Manual)

Malicious Applets:
Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system. (SOURCE: CNSSI-4009)

Malicious Code:
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (SOURCE: NIST SP 800-53; CNSSI-4009)

Malicious Logic:
Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. (SOURCE: CNSSI-4009)

Malware:
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (SOURCE: NIST SP 800-83)

See Malicious Code. See also Malicious Applets and Malicious Logic.
(SOURCE: NIST SP 800-53; CNSSI-4009)

A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
(SOURCE: NIST SP 800-61)

Man-in-the-middle Attack (MitM):
An attack on the authentication protocol run in which the Attacker positions himself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.
(SOURCE: NIST SP 800-63)

A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (SOURCE: CNSSI-40090)

Management Controls:
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; FIPS 200)

Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions. (SOURCE: CNSSI-4009)

Management Security Controls:
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security. (SOURCE: CNSSI-4009)

Mandatory Access Control (MAC):
A means of restricting access to system resources based on the sensitivity (as represented by a label) of the information contained in the system resource and the formal authorization (i.e., clearance) of users to access information of such sensitivity. (SOURCE: NIST SP 800-44; CNSSI-4009)

Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information. (SOURCE: FIPS 191)

Masking:
In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed. See Truncation for protection of PAN when stored in files, databases, etc. (SOURCE: PCI DSS GLOSSARY)

Masquerading:
When an unauthorized agent claims the identity of another agent, it is said to be masquerading. (SOURCE: NIST SP 800-19)

A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. (SOURCE: CNSSI-4009)

Maximum Tolerable Downtime (MTD):
The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission. (SOURCE: NIST SP 800-34)

Media:
Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (SOURCE: FIPS 200; NIST SP 800-53; CNSSI-4009)

Media Sanitization:
A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (SOURCE: NIST SP 800-88)

The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (SOURCE: CNSSI-4009)

Memorandum of Understanding/Agreement (MOU/A):
A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (SOURCE: NIST SP 800-47; CNSSI-4009)

Memory-Scraping Attacks:
Malware activity that examines and extracts data that resides in memory as it is being processed or which has not been properly flushed or overwritten. (SOURCE: PCI DSS GLOSSARY)

Message Authentication Code (MAC):
A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. MACs provide authenticity and integrity protection, but not non- repudiation protection. (SOURCE: NIST SP 800-63; FIPS 201)

A cryptographic checksum that results from passing data through a message authentication algorithm. (SOURCE: FIPS 198)

Metadata:
Data about data. The definition and scope of metadata depends upon context. In the context of Information Management, metadata is generally thought of as providing information (what database stores it? what data type is it? how long is the field? etc.) about a data element. Within the context of Data Governance, the term also includes “business” metadata such as the names and roles of Data Stewards. Metadata repositories are employed to store and report on metadata. (SOURCE: Data Governance Institute)

MIME:
See Multipurpose Internet Mail Extensions.

Minor Application:
An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system. (SOURCE: NIST SP 800-18)

Mobile Application Management (MAM):
Mobile Application Management (MAM) and Mobile Application Store (MAS) management perform application monitoring, reporting, security, and deployment. (SOURCE: GSA.gov)

Mobile Code:
Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. (SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009)

A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
(SOURCE: NIST SP 800-28)

Mobile Device:
For the purposes of the Mobile Device Management Policy included in this Manual, a Mobile Device is any smartphone or tablet device that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.
(SOURCE: State of New Hampshire Statewide Information Security Manual)

Other definitions of a Mobile Device include:
Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory).

Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (SOURCE: NIST SP 800-53)

Mobile Device Management (MDM):
Mobile device management (MDM) is software that allows IT administrators to control, secure and enforce policies on smartphones, tablets and other endpoints. (SOURCE: whatis.com)

Mode of Operation:
An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm. (SOURCE: NIST SP 800-38C)

Description of the conditions under which an information system operates based on the sensitivity of information processed and the clearance levels, formal access approvals, and need-to-know of its users. Four modes of operation are authorized for processing or transmitting information: dedicated mode, system high mode, compartmented/partitioned mode, and multilevel mode. (SOURCE: CNSSI-4009)

Moderate Impact:
The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States i.e.
Causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
Results in significant damage to organizational assets;
Results in significant financial loss; or
Results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

(SOURCE: CNSSI-4009)

Multi-Homed Connection:
A host connected to two or more networks or having two or more network addresses. For example, a computer may be connected to multiple Local Area Networks (LANs).
(SOURCE: State of New Hampshire Statewide Information Security Manual)

Multi-Protocol Label Switching (MPLS):
A standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multi-protocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS).
(SOURCE: Method and System for Detecting A Connection Fault)

Multifactor Authentication:
Authentication using two or more factors to achieve authentication. Factors include:
something you know (e.g., password/PIN);
something you have (e.g., cryptographic identification device, token); or
something you are (e.g., biometric). See Authenticator.
(SOURCE: NIST SP 800-53)

Multiprotocol Label Switching (MPLS):
A mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL. (SOURCE: Wikipedia)

Multipurpose Internet Mail Extensions (MIME):
An Internet standard that extends the format of email to support:
Text in character sets other than ASCII
Non-text attachments
Message bodies with multiple parts
Header information in non-ASCII character sets
Although MIME was designed mainly for SMTP protocol, its use today has grown beyond describing the content of email and now often includes descriptions of content type in general, including for the web (see Internet media type) and as a storage for rich content in some commercial products. Virtually all human-written Internet email and a large proportion of automated email are transmitted via SMTP in MIME format. Internet email is so closely

associated with the SMTP and MIME standards that it is sometimes called SMTP/MIME email. (SOURCE: Wikipedia)

Mutual Authentication:
Occurs when parties at both ends of a communication activity authenticate each other. (SOURCE: NIST SP 800-32)

The process of both entities involved in a transaction verifying each other. (SOURCE: CNSSI-4009)

NIST – NULL

National Institute of Standards and Technology:
A measurement standards laboratory that is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to: Promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

The Information Technology Laboratory (ITL), one of several components within NIST, publishes standards concerning information security. (SOURCE: Wikipedia)

Need-To-Know:
A method of isolating information resources based on a user's need to have access to that resource to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (SOURCE: CNSSI-4009)

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: NIST SP 800-53; CNSSI-4009)

Network Access:
Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (SOURCE: NIST SP 800-53; CNSSI-4009)

Network Access Control (NAC):
A feature provided by some firewalls that allows access based on a user's credentials and the results of health checks performed on the telework client device. (SOURCE: NIST SP 800-41)

Network Address Translation (NAT):
A routing technology used by many firewalls to hide internal system addresses from an external network through use of an addressing schema. (SOURCE: NIST SP 800-41)

Network Resilience:
A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. (SOURCE: CNSSI-4009)

Network Security Scan:
Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals. (SOURCE: PCI DSS GLOSSARY)

Network Sniffing:
A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique. (SOURCE: NIST SP 800-115)

Network Time Protocol (NTP):
A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. (SOURCE: Wikipedia)

Network Weaving:
Penetration technique in which different communication networks are linked to access an information system to avoid detection and trace- back. (SOURCE: CNSSI-4009)

Network-attached Storage (NAS):
A file-level computer data storage connected to a computer network providing data access to a heterogeneous group of clients. (SOURCE: Wikipedia)

Network-Level Connection:
The connection provides access to a State Agency's private network through tunneling or a remote desktop access architecture and the software and data that reside on the internal information assets. (SOURCE: State of New Hampshire Statewide Information Security Manual)

Non-Console Access:
Refers to logical access to a system component that occurs over a network interface rather than via a direct, physical connection to the system component. Non-console access includes access from within local/internal networks as well as access from external, or remote, networks.
(SOURCE: Payment Card Industry Data Security Standards (PCI-DSS))

Nonpublic Information:
Information that the employee obtains, or is provided access to, during his/her employment with

the State of New Hampshire that the employee knows, or reasonably should know, has not been made available to the public. It includes information that the employee knows, or reasonably should know:
Is designated by the State or the Agency for which the Employee works as nonpublic information;
Contains markings such as “Confidential”, “Internal”, “Restricted”, or similar language, or is considered sensitive information;
Contains information that must be protected by State or Federal Statute, State or Agency policy, or other regulation;
Is provided to the State or the Agency for which the employee works by customers or third parties under agreement and with the understanding that it will be treated as confidential, nonpublic information; or
Contains information related to the internal State or Agency capabilities and operations that is not available to the public, or that an individual could use to negotiate or otherwise circumvent security controls. (SOURCE: State of New Hampshire Statewide Information Security Manual)

Non-Repudiation:
Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. (SOURCE: CNSSI-4009; NIST SP 800-60)

Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.
(SOURCE: NIST SP 800-53; NIST SP 800-18)

It is the security service by which the entities involved in a communication cannot deny having participate. Specifically, the sending entity cannot deny having sent a message (non-repudiation with proof of origin), and the receiving entity cannot deny having received a message (non-repudiation with proof of delivery). (SOURCE: FIPS 191)

A service that is used to provide assurance of the integrity and origin of data 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 (i.e., the signatory). (SOURCE: FIPS 186)

Null:
Dummy letter, letter symbol, or code group inserted into an encrypted message to delay or prevent its decryption or to complete encrypted groups for transmission or transmission security purposes. (SOURCE: CNSSI-4009)

OBJECT – OVERWRITE PROCEDURE

Object:
A passive entity that contains or receives information. (SOURCE: NIST SP 800-27)

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains. (SOURCE: CNSSI-4009; NIST SP 800-53)

Off-line Attack:
An attack where the Attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing. (SOURCE: NIST SP 800-63)

One-Way Hash Algorithm:
Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed-size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature). (SOURCE: NIST SP 800-49; CNSSI-4009)

Online Attack:
An attack against an authentication protocol where the Attacker either assumes the role of a Claimant with a genuine Verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets. (SOURCE: NIST SP 800-63)

Open Shortest Path First (OSPF):
A link-state routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). (SOURCE: Wikipedia)

Open Web Application Security Project (OWASP):
A non-profit organization focused on improving the security of application software. OWASP maintains a list of critical vulnerabilities for web applications. (SOURCE: PCI DSS GLOSSARY)

Operational Technology:
The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term has become established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment. (SOURCE: Wikipedia)

Organizational Information Security Continuous Monitoring:
Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data-driven risk management decisions. (SOURCE: NIST SP 800-137)

Outside Threat:
An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. (SOURCE: NIST SP 800-32)

Overwrite Procedure:
A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns. (SOURCE: CNSSI-4009)

PACKET FILTER – PUBLIC KEY INFRASTRUCTURE (PKI)

Packet Filter:
A routing device that provides access control functionality for host addresses and communication sessions. (SOURCE: NIST SP 800-41)

Packet Sniffer:
Software that observes and records network traffic. (SOURCE: CNSSI-4009)

Parity:
Bit(s) used to determine whether a block of data has been altered. (SOURCE: CNSSI-4009)

Partitioning:
A file format in which the file is divided into multiple sub files and a directory is established to locate each sub file. (SOURCE: ISACA)

Passive Attack:
An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping). (SOURCE: NIST SP 800-63)

An attack that does not alter systems or data. (SOURCE: CNSSI-4009)

Passive Security Testing:
Security testing that does not involve any direct interaction with the targets, such as sending packets to a target. (SOURCE: NIST SP 800-115)

Password:
A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. (SOURCE: NIST SP 800-63)

A protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. (SOURCE: FIPS 181)

A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (SOURCE: FIPS 140-2)

A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. (SOURCE: CNSSI-4009)

Password Cracking:
The process of recovering secret passwords stored in a computer system or transmitted over a network. (SOURCE: NIST SP 800-115)

Password Protected:
The ability to protect a file using a password access control, protecting the data contents from being viewed with the appropriate viewer unless the proper password is entered. (SOURCE: NIST SP 800-72)

The ability to protect the contents of a file or device from being accessed until the correct password is entered. (SOURCE: NIST SP 800-124)

Patch:
An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (SOURCE: NIST SP 800-123)

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)

Payment Card Industry (PCI):
The term refers to the Payment Card Industry Security Standards Council, a council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The PCI Council formed a body of security standards known as the PCI Data Security Standards, (PCI DSS), and these standards consist of 12 significant requirements including multiple sub-requirements that contain numerous directives against which businesses may measure their own payment card security policies, procedures and guidelines. By complying with qualified

assessments of these standards, businesses can become accepted by the PCI Standards Council as compliant with the 12 requirements, and thus receive a compliance certification and a listing on the PCI Standards Council website. Compliance efforts and acceptance must be completed on a periodic basis.
(SOURCE: Wikipedia)

Payment Card Industry Data Security Standard (PCI DSS):
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. (SOURCE: Wikipedia)

Private Branch Exchange (PBX):
A telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

Penetration Testing:
A test methodology in which assessors, using all available documentation (e.g., system design, (SOURCE code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. (SOURCE: NIST SP 800-53A; NIST SP 800-53; CNSSI-4009)

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. (SOURCE: NIST SP 800-115)

Perishable Data:
Information whose value can decrease substantially during a specified time. A significant decrease in value occurs when the operational circumstances change to the extent that the information is no longer useful. (SOURCE: CNSSI-4009)

Personal Firewall:
A utility on a computer that monitors network activity and blocks communications that are unauthorized. (SOURCE: NIST SP 800-69)

Personal Identification Number (PIN):
A password consisting only of decimal digits. (SOURCE: NIST SP 800-63)

A secret that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits. (SOURCE: FIPS 201)

An alphanumeric code or password used to authenticate an identity. (SOURCE: FIPS 140-2)

A short numeric code used to confirm identity. (SOURCE: CNSSI-4009)

Personal Information (PI):
An individual's first name or first initial and last name linked with any one or more of the following data elements:
Social Security number;
Driver's license number or State identification card number; or
Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. [N.J.S.A. 2C:56:8-161]

“Personal Information” as defined by N.J.S.A. 39:2-3.3 “Personal Information” means information that identifies an individual, including an individual’s photograph; social security number; driver identification number; name; address other than the five-digit zip code; telephone number; and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status. [N.J.S.A. 39:2-3.3]

Personally Identifiable Information (PII):
Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. (SOURCE: CNSSI-4009)

Any information about an individual maintained by an agency, including

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

(SOURCE: NIST SP 800-122)

Phishing:
Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. (SOURCE: NIST SP 800-83)

Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means. (SOURCE: CNSSI-4009)

A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.
(SOURCE: NIST SP 800-115)

PII Confidentiality Impact Level:
The PII confidentiality impact level—low, moderate, or high— indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. (SOURCE: NIST SP 800-122)

Plaintext:
Data input to the Cipher or output from the Inverse Cipher. (SOURCE: FIPS 197)

Intelligible data that has meaning and can be understood without the application of decryption. (SOURCE: NIST SP 800-21)

Unencrypted information. (SOURCE: CNSSI-4009)

Platform as a Service:
The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages 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 application hosting environment configurations. (SOURCE: Cloud Security Alliance)

Policy-Based Access Control (PBAC):
A form of access control that uses an authorization policy that is flexible in the types of evaluated parameters (e.g., identity, role, clearance, operational need, risk, and heuristics). (SOURCE: CNSSI-4009)

Port Scanning:
Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). (SOURCE: CNSSI-4009)

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

Portability:
Usability of the same software in different IT environments. The pre-requirement for portability is the generalized abstraction between the application logic and system interfaces. When software with the same functionality is produced for several computing platforms, portability is the key issue for development cost reduction. (SOURCE: Wikipedia)

Portable Document Format (PDF):
A file format used to present documents in a manner independent of application software, hardware, and operating systems. (SOURCE: Wikipedia)

Portal:
A high-level remote access architecture that is based on a server that offers teleworkers access to one or more applications through a single centralized interface. (SOURCE: NIST SP 800-46)

Post Office Protocol v3 (POP3):
Application-layer protocol used by e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. (SOURCE: PCI DSS GLOSSARY)

Potential Impact:
The loss of confidentiality, integrity, or availability could be expected to have:
A limited adverse effect (FIPS 199 low);
A serious adverse effect (FIPS 199 moderate); or
A severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
(SOURCE: NIST SP 800-53; NIST SP 800-60; NIST SP 800-37; FIPS 199)

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect; a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. (SOURCE: FIPS 200; CNSSI-4009)

Precursor:
A sign that an attacker may be preparing to cause an incident. (SOURCE: NIST SP 800-61; CNSSI-4009)

Predisposing Condition:
A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation. (SOURCE: NIST SP 800-30)

Print Suppression:
Eliminating the display of characters in order to preserve their secrecy. (SOURCE: CNSSI-4009)

Privacy:
Restricting access to subscriber or Relying Party information in accordance with federal law and agency policy. (SOURCE: NIST SP 800-32)

Freedom from unauthorized intrusion or disclosure of information about an individual (SOURCE: ISACA)

Privacy Impact Assessment (PIA):
An analysis of how information is handled:

to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and
to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
(SOURCE: NIST SP 800-53; NIST SP 800-18; NIST SP 800-122; CNSSI-4009; OMB Memorandum 03-22)

Private Key:
The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. (SOURCE: NIST SP 800-63)

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to:
Compute the corresponding public key,
Compute a digital signature that may be verified by the corresponding public key,
Decrypt keys that were encrypted by the corresponding public key, or
Compute a shared secret during a key-agreement transaction.
(SOURCE: NIST SP 800-57 Part 1; FIPS 196; FIPS 140-2)

In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. (SOURCE: CNSSI-4009)

Private Network:
Network established by an organization that uses private IP address space. Private networks are commonly designed as local area networks. Private network access from public networks should be properly protected with the use of firewalls and routers. (SOURCE: PCI DSS GLOSSARY)

Privilege:
A right granted to an individual, a program, or a process. (SOURCE: CNSSI-4009)

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

Privileged User:
A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform. (SOURCE: NIST SP 800-53; CNSSI-4009)

Probe:
A technique that attempts to access a system to learn something about the system.
(SOURCE: CNSSI-4009)

Problem:
A cause of one or more incidents. (SOURCE: ITIL V3)

Process:
A structured set of activities designed to accomplish a specific objective. A process takes one or more defined inputs and turns them into defined outputs. (SOURCE: ITIL V3)

Include formal and informal mechanisms (large and small, simple and complex) to accomplish objectives. Processes identify, measure, manage, and control risks to confidentiality, integrity, availability, privacy, and safety, and they also ensure accountability. (SOURCE: ISACA Business Model for Information Security)

Process Manager:
An individual accountable for operational management of a process. There may be several process managers for one process and the process manager role is often assigned to the same person carrying out the process owner role. (SOURCE: ITIL V3)

Programmable Logic Controller (PLC) or Programmable Controller:
An industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires

high reliability control and ease of programming and process fault diagnosis. (SOURCE: Wikipedia)

Promiscuous Mode:
A configuration setting for a network interface card that causes it to accept all incoming packets that it sees, regardless of their intended destinations. (SOURCE: NIST SP 800-94)

Protected Health Information:
The term Protected Health Information is composed from two definitions in Section 1171 of Part C of Subtitle F of Public Law 104-191 (August 21, 1996): Health Insurance Portability and Accountability Act of 1996: Administrative Simplification. These statutory definitions are of health information and individually identifiable health information.

> **Health information** means any information, whether oral or recorded in any form or medium, that:

is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

> **Individually Identifiable Health Information** is information that is a subset of health information, including demographic information collected from an individual, and:

Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

That identifies the individual; or

With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

> Protected Health Information means individually identifiable health information [defined above]:
>
> > Except as provided in paragraph (b) of this definition, that is:
> >
> > > Transmitted by electronic media;
> > >
> > > Maintained in electronic media; or
> > >
> > > Transmitted or maintained in any other form or medium.
> >
> > Protected health information excludes individually identifiable health information in:

Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

Employment records held by a covered entity in its role as employer.

The HIPAA Privacy Rule covers protected health information in any medium while the HIPAA Security Rule covers electronic protected health information.

With those definitions in place, the question becomes: what elements comprise protected health information such that if they were removed, items (i) and (ii) of (b) in the definition of individually identifiable health information would not obtain. The answer is in the de-identification standard and its two implementation specifications of the HIPAA Privacy Rule [45 CFR 164.514]:

(a) Standard: de-identification of protected health information. Health information [defined above] that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information; and

Documents the methods and results of the analysis that justify such determination; or

The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

Names;

All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Censue:

The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

Telephone numbers;

Fax numbers;

Electronic mail addresses;

Social security numbers;

Medical record numbers;

Health plan beneficiary numbers;

Account numbers;

Certificate/license numbers;

Vehicle identifiers and serial numbers, including license plate numbers;

Device identifiers and serial numbers;

Web Universal Resource Locators (URLs);

Internet Protocol (IP) address numbers;

Biometric identifiers, including finger and voice prints;

Full face photographic images and any comparable images; and

Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(SOURCE: HIPAA)

Protocol:
Set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (SOURCE: CNSSI-4009)

Proxy:
A proxy is an application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for email.
(SOURCE: NIST SP 800-44; CNSSI-4009)

Proxy Agent:
A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device. (SOURCE: CNSSI-4009)

Proxy Server:
A server that services the requests of its clients by forwarding those requests to other servers.
(SOURCE: CNSSI-4009)

Public Key (Asymmetric) Cryptographic Algorithm:
A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.
(SOURCE: FIPS 140-2)

Public Key:
The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. (SOURCE: FIPS 201; NIST SP 800-63)

A cryptographic key, used with a public key cryptographic algorithm that is uniquely associated with an entity and may be made public. In an asymmetric (public) cryptosystem, the public key is associated with a private key. The public key may be known by anyone and, depending on the algorithm, may be used, for example, to:
Verify a digital signature that is signed by the corresponding private key,
Encrypt keys that can be decrypted by the corresponding private key, or
Compute a shared secret during a key-agreement transaction.
(SOURCE: NIST SP 800-57 Part 1; FIPS 196; FIPS 140-2; CNSSI-4009

Public Key Certificate:
A digital document issued and digitally signed by the private key of a Certificate authority that binds the name of a Subscriber to a public key. The certificate indicates that the Subscriber

identified in the certificate has sole control and access to the private key. (SOURCE: NIST SP 800-63)

A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority). (SOURCE: FIPS 196)

A set of data that uniquely identifies an entity, contains the entity's public key, and is digitally signed by a trusted party, thereby binding the public key to the entity. (SOURCE: FIPS 140-2)

Public Key Infrastructure (PKI):
A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. (SOURCE: NIST SP 800-32; NIST SP 800-63)

An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys. (SOURCE: FIPS 196)

A Framework that is established to issue, maintain, and revoke public key certificates.
(SOURCE: FIPS 186)

A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system. (SOURCE: FIPS 201)

The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. (SOURCE: CNSSI-4009)

QUALITIY OF SERVICE – RULE-BASED SECURITY TESTING

Quality of Service (QoS):
The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service-Level Agreement between a user and a service provider, to satisfy specific customer application requirements. Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.
(SOURCE: CNSSI-4009)

Rainbow Table Attack:
A method of data attack using a pre-computed table of hash strings (fixed-length message digest) to identify the original data (SOURCE, usually for cracking password or cardholder data hashes. (SOURCE: PCI DSS GLOSSARY)

Reciprocity:
Agreement among participating enterprises to accept each other's security assessments to reuse information system resources and/or to accept each other's assessed security posture to share information.
(SOURCE: CNSSI-4009; NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-39)

Records:
The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on items). (SOURCE: NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. [44 U.S.C. SEC. 3301] (SOURCE: FIPS 200)

Records Management:
The process for tagging information for records-keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements. (SOURCE: CNSSI-4009)

Recovery Point Objective (RPO):
The point in time to which data must be recovered after an outage. (SOURCE: NIST SP 800-34)

Recovery Procedures:
Actions necessary to restore data files of an information system and computational capability after a system failure. (SOURCE: CNSSI-4009)

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: SP800-34)

Red Team:
A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. (SOURCE: CNSSI 4009-2015)

Remanence:
Residual information remaining on storage media after clearing. See Magnetic Remanence and Clearing. (SOURCE: CNSSI-4009)

Remediation:
The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. (SOURCE: NIST SP 800-40)

The act of mitigating a vulnerability or a threat. (SOURCE: CNSSI-4009)

Remediation Plan:
A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation. (SOURCE: NIST SP 800-40)

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 800-53)

Access by users (or information systems) communicating external to an information system security perimeter. (SOURCE: NIST SP 800-18)

The ability for an organization's users to access its nonpublic computing resources from external locations other than the organization's facilities. (SOURCE: NIST SP 800-46)

Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). (SOURCE: CNSSI-4009)

Remote Desktop Access Architecture:
A high-level remote access architecture that gives a user the ability to remotely control a particular computer at their agency from an external network. Remote desktop access architecture includes, but is not limited to, systems (local and remote) and software (e.g., Cisco AnyConnect, Citrix, GoToMyPC, Verisign Identity Protection (VIP)) that is used to facilitate and

secure the remote session. The specific technologies utilized in a remote desktop access architecture are determined by the New Hampshire Office of Information Technology. (SOURCE: State of New Hampshire Statewide Information Security Manual)

Removable Media:
Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), thumb drives, pen drives, and similar USB storage devices. (SOURCE: CNSSI-4009; NIST SP 800-53)

Replay Attacks:
An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. (SOURCE: CNSSI-4009)

Report on Compliance (ROC):
Report documenting detailed results from an entity's PCI DSS assessment.
(SOURCE: PCI DSS GLOSSARY)

Repository:
A database containing information and data relating to certificates as specified in a CP; may also be referred to as a directory. (SOURCE: NIST SP 800-32)

Representational State Transfer (REST):
A software architectural style consisting of a coordinated set of architectural constraints applied to components, connectors, and data elements, within a distributed hypermedia system. REST ignores the details of component implementation and protocol syntax in order to focus on the roles of components, the constraints upon their interaction with other components, and their interpretation of significant data elements. (SOURCE: Wikipedia)

Residual Risk:
The remaining potential risk after all IT security measures are applied. There is a residual risk associated with each threat. (SOURCE: NIST SP 800-33)

Portion of risk remaining after security measures have been applied.
(SOURCE: CNSSI-4009; NIST SP 800-30)

Residue:
Data left in storage after information-processing operations are complete, but before degaussing or overwriting has taken place. (SOURCE: CNSSI-4009)

Resilience:
The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. (SOURCE: NIST SP 800-34)

The ability to continue to:
operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and
recover to an effective operational posture in a time frame consistent with mission needs.
(SOURCE: NIST SP 800-137)

Risk:
The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
(SOURCE: FIPS 200; NIST SP 800-60)

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
The adverse impacts that would arise if the circumstance or event occurs; and
The likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
(SOURCE: NIST SP 800-37; NIST SP 800-53A NIST SP 800-53; CNSSI-4009

Risk Analysis:
The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. (SOURCE: NIST SP 800-27)

Examination of information to identify the risk to an information system. See Risk Assessment. (SOURCE: CNSSI-4009)

Risk Assessment:
The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37)

The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). (SOURCE: CNSSI-4009)

Risk Management:
The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:
The conduct of a risk assessment;
The implementation of a risk mitigation strategy; and
Employment of techniques and procedures for the continuous monitoring of the security state of the information system.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009; NIST SP 800-82; NIST SP 800-34)

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:
The conduct of a risk assessment;
The implementation of a risk mitigation strategy; and
Employment of techniques and procedures for the continuous monitoring of the security state of the information system.
(SOURCE: FIPS 200)

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. (SOURCE: NIST SP 800-39)

Risk Mitigation:
Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
(SOURCE: CNSSI-4009; NIST SP 800-30; NIST SP 800-39)

Risk Monitoring:
Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. (SOURCE: NIST SP 800-30; NIST SP 800-39)

Risk Tolerance:
The level of risk an entity is willing to assume in order to achieve a potential desired result. (SOURCE: NIST SP 800-32)

The defined impacts to an enterprise's information systems that an entity is willing to accept. (SOURCE: CNSSI-4009)

Rogue Device:
An unauthorized node on a network. (SOURCE: NIST SP 800-115)

Role:
A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. (SOURCE: CNSSI-4009)

Role-Based Access Control (RBAC):
A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. (SOURCE: NIST SP 800-95)

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
(SOURCE: NIST SP 800-53; CNSSI-4009)

Root Cause Analysis:
A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks. (SOURCE: NIST SP 800-30; NIST SP 800-39)

Router:
Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways. (SOURCE: PCI DSS GLOSSARY)

Rule-Based Security Policy:
A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. (SOURCE: NIST SP 800-33; CNSSI-4009)

S/MIME – SYSTEM SOFTWARE

S/MIME (NIST)
A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).
(SOURCE: NIST SP 800-49)

Safeguards:
Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
(SOURCE: NIST SP 800-53; NIST SP 800-37; FIPS 200; CNSSI-4009)

Safety:
Condition of being protected from harm or other non-desirable outcomes. (SOURCE: Wikipedia)

Sanitization:
Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. (SOURCE: FIPS 200)

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. (SOURCE: NIST SP 800-53; CNSSI-4009)

Scalability:
The ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. (SOURCE: WIKIPEDIA

Scanning:
Sending packets or requests to another system to gain information to be used in a subsequent attack. (SOURCE: CNSSI-4009)

Scoping:
Process of identifying all system components, people, and processes to be included in an assessment. The first step of an assessment is to accurately determine the scope of the review.
(SOURCE: PCI DSS GLOSSARY)

Secret Key:
A cryptographic key that is used with a secret-key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term "secret" in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. (SOURCE: NIST SP 800-57)

A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term "secret" in this context does not imply a classification level, but rather implies the need to protect the key from disclosure.
(SOURCE: CNSSI-4009)

A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution. (SOURCE: FIPS 201)

A cryptographic key that is uniquely associated with one or more entities. The use of the term "secret" in this context does not imply a classification level, but rather implies the need to protect the key from disclosure or substitution. (SOURCE: FIPS 198)

A cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. (SOURCE: FIPS 140-2)

Secure Coding Guidelines:
Philosophy and approach supporting the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities. Defects, bugs and logic flaws are consistently the primary cause of commonly exploited software vulnerabilities. Through the analysis of thousands of reported vulnerabilities, security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. By identifying the insecure coding practices that lead to these errors and educating developers on secure alternatives, organizations can take proactive steps to help significantly reduce or eliminate vulnerabilities in software before deployment. (SOURCE: Wikipedia)

Secure DNS (SECDNS):
Configuring and operating DNS servers so that the security goals of data integrity and (SOURCE authentication are achieved and maintained. (SOURCE: NIST SP 800-81)

Secure Hash Algorithm (SHA):
A hash algorithm with the property that is computationally infeasible
To find a message that corresponds to a given message digest, or
To find two different messages that produce the same message digest.
(SOURCE: CNSSI-4009)

Secure Hash Standard:
This Standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed representation of electronic data (message). When a message of any length less than 2^64 bits (for SHA-1, SHA-224 and SHA-256) or less than 2^128 bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

The hash algorithms specified in this Standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm. (SOURCE: FIPS 180-4)

Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. (SOURCE: CNSSI-4009)

Secure Shell (SSH):
Protocol suite providing encryption for network services like remote login or remote file transfer. (SOURCE: PCI DSS GLOSSARY)

Secure Socket Layer (SSL):
A protocol used for protecting private information during transmission via the Internet.

Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:” (SOURCE: CNSSI-4009)

Security:
A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach. (SOURCE: CNSSI-4009)

Security Assertion Markup Language (SAML):
An XML-based security specification developed by the Organization for the Advancement of Structured Information Standards (OASIS) for exchanging authentication (and authorization) information between trusted entities over the Internet. (SOURCE: NIST SP 800-63)

A framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called “assertions,” enhancing the interoperability between disparate applications. (SOURCE: NIST SP 800-95)

A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between online business partners. (SOURCE: CNSSI-4009)

Security Attribute:
A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. (SOURCE: FIPS 188)

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy. (SOURCE: NIST SP 800-53; CNSSI-4009)

Security Content Automation (SCAP):
A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements. (SOURCE: CNSSI-4009)

Security Control Assessment:
The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

Security Control Baseline:
The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system. (SOURCE: NIST SP 800-53; FIPS 200)

One of the sets of minimum-security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253. (SOURCE: NIST SP 800-53A)

Security Control Effectiveness:
The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance. (SOURCE: NIST SP 800-137)

Security Controls:
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
(SOURCE: NIST SP 800-53; NIST SP 800-37; NIST SP 800-53A; NIST SP 800-60; FIPS 200; FIPS 199; CNSSI-4009)

Security Controls Baseline:
The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system. (SOURCE: CNSSI-4009)

Security Domain:
A set of subjects, their information objects, and a common security policy. (SOURCE: NIST SP 800-27)

A collection of entities to which applies a single security policy executed by a single authority. (SOURCE: FIPS 188)

A domain that implements a security policy and is administered by a single authority. (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-4009)

Security Impact Analysis:
The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

Security Information and Event Management (SIEM) Tool:
Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface. (SOURCE: NIST SP 800-128)

Security Objective:
Confidentiality, integrity, or availability.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-60; NIST SP 800-37; FIPS 200; FIPS 199)

Security Plan:
Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned

for meeting those requirements. See 'System Security Plan' or 'Information Security Program Plan.'
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-18)

Security Policy:
The statement of required protection of the information objects. (SOURCE: NIST SP 800-27)

A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility to maintain a condition of security for systems and data.
(SOURCE: FIPS 188; (SOURCE: NIST SP 800-37; NIST SP 800-53; CNSSI-4009)

Security Requirements:
Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
(SOURCE: FIPS 200; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

Security Safeguards:
Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. (SOURCE: CNSSI-4009)

Security Test & Evaluation (ST&E):
Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system. (SOURCE: CNSSI-4009)

Security Testing:
Process to determine that an information system protects data and maintains functionality as intended. (SOURCE: CNSSI-4009)

Sensitive Data:
Data that is private, personal, or proprietary and must be protected from unauthorized access. (SOURCE: Data Governance Institute)

Sensitive Information:
A term to describe any information which requires protection from unauthorized access or disclosure. (SOURCE: State of New Hampshire Statewide Information Security Manual)

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

Sensitivity:
The degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components.

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

Service:
A capability provided by an information system that facilitates information processing, storage, or transmission. Also referred to as an information system service.

Service Management:
A set of specialized organizational capabilities for providing value to customers in the form of services. (SOURCE: ITIL V3)

Service Organization Control (SOC) - 1 Report:
These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, are specifically intended to meet the needs of the managements of user entities and the user entities' auditors, as they evaluate the effect of the controls at the service organization on the user entities' financial statement assertions. These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of comply with laws and regulations such as the Sarbanes-Oxley Act and the user entities' auditors as they plan and perform audits of the user entities' financial statements. There are two types of reports for these engagements:

Type 1 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.

Type 2 – report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

The use of these reports is restricted to the management of the service organization, user entities of the service organization and user auditors. (SOURCE: AICPA Website)

Service Organization Control (SOC) - 2 Report:
These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service organization uses to process users' data and

the confidentiality and privacy of the information processed by these systems . Examples of stakeholders who may need these reports are, management or those charged with governance of the user entities and of the service organization, customers of the service organization, regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls. Use of these reports generally is restricted to parties that have this understanding The AICPA Guide: Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (currently under development) provides guidance for performing these engagements. These reports can play an important role in:

Oversight of the organization

Vendor management programs

Internal corporate governance and risk management processes

Regulatory oversight

Similar to a SOC 1 report there are two types of report: A type 2, report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls; and a type 1, report on management's description of a service organization's system and the suitability of the design of controls. Use of these reports is generally restricted.
(SOURCE: AICPA Website)

Service Organization Control (SOC) - 3 Report:
These reports are designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems used by a service organization to process users' information, and the confidentiality, or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report.

These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 reports can be freely distributed or posted on a website as a SysTrust for Service Organizations seal. For more information about the SysTrust for Service Organization seal program go to www.webtrust.org.
(SOURCE: AICPA Website)

Service Oriented Architecture (SOA):
An architectural style and discipline that improves IT's ability to meet business demands. Service-oriented design principles advocate factoring system capabilities into loosely coupled, autonomous components (i.e., services) and making the capabilities available to other system components or external consumers. SOA is not dependent on any particular technology.
(SOURCE: The Burton Group (Gartner))

Service-Level Agreement (SLA):
Defines the specific responsibilities of the service provider and sets the customer expectations. (SOURCE: CNSSI-4009)

Session:
A semi-permanent interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user (see Login session). A session is set up or established at a certain point in time, and then torn down at some later point. An established communication session may involve more than one message in each direction. A session is typically, but not always, stateful, meaning that at least one of the communicating parts needs to save information about the session history in order to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses. (SOURCE: Wikipedia)

Session Initiation Protocol (SIP):
A signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks. The protocol defines the messages that are sent between endpoints that govern establishment, termination and other essential elements of a call. SIP can be used for creating, modifying and terminating sessions consisting of one or several media streams. SIP can be used for two-party (unicast) or multiparty (multicast) sessions. Other SIP applications include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer, fax over IP and online games. (SOURCE: Wikipedia)

Signature:
A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.
(SOURCE: NIST SP 800-61; CNSSI-4009)

Signature Certificate:
A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
(SOURCE: NIST SP 800-32; CNSSI-4009)

Signed Data:
Data on which a digital signature is generated. (SOURCE: FIPS 196)

Simple Mail Transfer Protocol (SMTP):
An Internet standard for electronic mail (e-mail) transmission. (SOURCE: Wikipedia)

Simple Network Management Protocol (SNMP):
An Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

It is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. (SOURCE: Wikipedia)

Simple Object Access Protocol (SOAP):
A protocol specification for exchanging structured information in the implementation of web services in computer networks. It relies on XML Information Set for its message format, and usually relies on other application layer protocols, most notably Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission. (SOURCE: Wikipedia)

Single Point of Failure:
A resource whose loss will result in the loss of service or production. (SOURCE: ISACA)

SLA:
Service Level Agreements - Defines the specific responsibilities of the service provider and sets the customer expectations. (SOURCE: NIST)

Smartphone:
A handheld mobile communication device with a mobile operating system and an integrated mobile broadband cellular network and Wi-Fi connection capability used for voice and data communications. (SOURCE: Wikipedia)

Social Engineering:
An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. (SOURCE: NIST SP 800-61; CNSSI-4009)

A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. (SOURCE: NIST SP 800-114)

The process of attempting to trick someone into revealing information (e.g., a password).
(SOURCE: NIST SP 800-115)

Social Media:
The interaction among people in which they create, share or exchange information and ideas in virtual communities and networks. (SOURCE: Wikipedia)

Social Networking:
Use of a platform/service to support collaboration among people who share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his social links, and a variety of additional services. Social networking

is web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools such as, mobile connectivity, photo/video/sharing and blogging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network. (SOURCE: Wikipedia)

Software:
Computer programs and associated data that may be dynamically written or modified during execution. (SOURCE: NIST)

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 a thin client interface such as a web browser (e.g., web-based email). 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: Cloud Security Alliance)

Software Development Life Cycle (SDLC):
Acronym for "system development life cycle" or "software development lifecycle." Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation. (SOURCE: PCI DSS GLOSARY)

Spam:
The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (SOURCE: NIST NIST SP 800-53)

Unsolicited bulk commercial email messages. (SOURCE: NIST NIST SP 800-45)

Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (SOURCE: CNSSI-4009)

Special Character:
Any non-alphanumeric character that can be rendered on a standard American-English keyboard. Use of a specific special character may be application-dependent. The list of special characters follows:

` ~ ! @ # $ % ^ & * ( ) _ + | } { " : ? > < [ ] \ ; ' , . / - =

(SOURCE: CNSSI-4009)

Specification:
An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system. (SOURCE: NIST SP 800-53A)

Spillage:
Security incident that results in the transfer of classified or CUI information onto an information system not accredited (i.e., authorized) for the appropriate security level. (SOURCE: CNSSI-4009)

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

Spoofing:
"IP spoofing" refers to sending a network packet that appears to come from a source other than its actual source. (SOURCE: NIST SP 800-48)

Spyware:
Software that covertly gathers user information through the user's Internet connection without the user's knowledge. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
(SOURCE: NIST SP 800-53; CNSSI-4009)

SQL Injection:
Form of attack on database-driven web site. A malicious individual executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization's host computers through the computer that is hosting the database. (SOURCE: PCI DSS GLOSSARY)

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

State:
Intermediate Cipher result that can be pictured as a rectangular array of bytes. (SOURCE: FIPS 197)

Stateful Inspection:
Also called "dynamic packet filtering." Firewall capability that provides enhanced security by keeping track of the state of network connections. Programmed to distinguish legitimate packets for various connections, only packets matching an established connection will be permitted by the firewall; all others will be rejected. (SOURCE: PCI DSS GLOSSARY)

Stateless Protocol:
A communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of request and response. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. Examples of stateless protocols include the Internet Protocol (IP) which is the foundation for the Internet, and the Hypertext Transfer Protocol (HTTP) which is the foundation of data communication for the World Wide Web. (SOURCE: Wikipedia)

Storage Area Network (SAN):
A dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system.
(SOURCE: Wikipedia)

Strong Authentication:
The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. (SOURCE: CNSSI-4009)

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

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

Structured Query Language (SQL):
Computer language used to create, modify, and retrieve data from relational database management systems. (SOURCE: PCI DSS GLOSSARY)

Subject Matter Expert (SME):
A person who is an authority in a particular area or topic. (SOURCE: Wikipedia)

Subscriber:
A party who receives a credential or token from a CSP (Credentials Service Provider) and becomes a claimant in an authentication protocol. (SOURCE: CNSSI-4009; NIST SP 800-63)

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

Supplier:
Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain. Includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) vendors; and (iii) product resellers. (SOURCE: NIST SP800-161)

Supply Chain:
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. (SOURCE: NIST SP 800-53; CNSSI-4009)

Symmetric Key:
A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. (SOURCE: NIST SP 800-63; CNSSI-4009)

A single cryptographic key that is used with a secret (symmetric) key algorithm.
(SOURCE: NIST SP 800-21 [2nd Ed])

System:
Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (SOURCE: CNSSI-4009)

A system is defined as a discrete set of information technologies including computer hardware, software, databases, etc., organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (SOURCE: NIST)

System Administrator:
A person who manages the technical aspects of a system. (SOURCE: NIST SP 800-40)

Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. (SOURCE: CNSSI-4009)

System Assets:
Any software, hardware, data, administrative, physical, communications, or personnel resource within an information system. (SOURCE: CNSSI-4009)

System Development Life Cycle (SDLC):
The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. (SOURCE: NIST SP 800-34; CNSSI-4009)

System Integrity:
The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
(SOURCE: NIST SP 800-27)

Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (SOURCE: CNSSI-4009)

System Level Object:
Anything on a system component that is required for its operation, including but not limited to database tables, stored procedures, application executables and configuration files, system configuration files, static and shared libraries and DLLs, system executables, device drivers and device configuration files, and third-party components. (SOURCE: PCI DSS GLOSSARY)

System Security Plan:
Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
(SOURCE: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-18; FIPS 200)

The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. (SOURCE: CNSSI-4009)

System Software:
The special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, associated programs, and data. (SOURCE: FIPS 140-2)

TABLET – TWO FACTOR AUTHENTICATION

Tablet:
An open-faced handheld mobile communication and computing device with a mobile operating system, a touchscreen display, and an integrated Wi-Fi network capability. In some cases, tablets include cellular network connection capability. Tablets resemble smartphones with the major differences being that tablets are not typically used for voice communications, and they are larger. (SOURCE: Tech Target)

Tabletop Exercise:
Test method that presents a limited simulation of a disruption, emergency, or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation.
(SOURCE: ISO 22399:2007)

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: NIST SP 800-37; NIST SP 800-53; NIST SP 800-53A; CNSSI-4009)

Tampering:
An intentional event resulting in modification of a system, its intended behavior, or data.
(SOURCE: CNSSI-4009)

Technical Non-Repudiation:
The contribution of public key mechanisms to the provision of technical evidence supporting a non-repudiation security service. (SOURCE: NIST SP 800-32)

Technology:
Composed of the tools, applications, and infrastructure that make processes more efficient. Technology implemented by people following processes allows for the State to meet its information security objectives. (SOURCE: ISACA)

Telephone Network Protocol (TELNET):
Typically used to provide user-oriented command line login sessions to devices on a network. User credentials are transmitted in clear text. (SOURCE: PCI DSS GLOSSARY)

Terminal Access Controller Access Control System (TACACS):
Remote authentication protocol commonly used in networks that communicates between a remote access server and an authentication server to determine user access rights to the network. This authentication method may be used with a token, smart card, etc., to provide two-factor authentication. (SOURCE: PCI DSS GLOSSARY)

Test:
A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time. (SOURCE: NIST SP 800-53A)

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

Threat:
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; NIST SP 800-60; NIST SP 800-37; CNSSI-4009; FIPS 200)

The potential source of an adverse event. (SOURCE: NIST SP 800-61)

Threat Assessment:
Formal description and evaluation of threat to an information system.
(SOURCE: NIST SP 800-53; NIST SP 800-18)

Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. (SOURCE: CNSSI-4009; NIST SP 800-53A)

Threat Event:
An event or situation that has the potential for causing undesirable consequences or impact.
(SOURCE: NIST SP 800-30)

Threat Monitoring:
Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security. (SOURCE: CNSSI-4009)

Threat Source:
The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent. (SOURCE: FIPS 200; NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; CNSSI-4009)

Timestamp:
A sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second. Typically refers to digital date and time information attached to digital data. (SOURCE: Wikipedia)

Token:
Something that the claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity. (SOURCE: NIST SP 800-63)

Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also Cryptographic Token. (SOURCE: CNSSI-4009)

Total Risk:
The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). (SOURCE: NIST SP 800-16)

Tracking Cookie:
A cookie placed on a user's computer to track the user's activity on different Web sites, creating a detailed profile of the user's behavior. (SOURCE: NIST SP 800-83)

Traffic Analysis:
A form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g., from the source and destination numbers, or frequency and length of the messages. (SOURCE: NIST SP 800-24)

The analysis of patterns in communications for the purpose of gaining intelligence about a system or its users. It does not require examination of the content of the communications, which may or may not be decipherable. For example, an adversary may be able to detect a signal from a reader that could enable it to infer that a particular activity is occurring (e.g., a shipment has arrived, someone is entering a facility) without necessarily learning an identifier or associated data. (SOURCE: NIST SP 800-98)

Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the (SOURCE(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. (SOURCE: CNSSI-4009)

Transmission Security – (TRANSEC):
Measures (security controls) applied to transmissions to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

Note: TRANSEC is that field of COMSEC that deals with the security of communication transmissions, rather than that of the information being communicated. (SOURCE: CNSSI-4009)

Transport Layer Security (TLS):
An authentication and security protocol widely implemented in browsers and Web servers. (SOURCE: NIST SP 800-63)

Trap Door:
A means of reading cryptographically protected information using private knowledge of weaknesses in the cryptographic algorithm used to protect the data.

In cryptography, one-to-one function that is easy to compute in one direction yet believed to be difficult to invert without special information. (SOURCE: CNSSI-4009)

Trojan Horse:
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (SOURCE: CNSSI-4009)

Trust Anchor:
A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. The trust anchor’s public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. (SOURCE: NIST SP 800-57 Part 1)

An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process [or person] loading the signed software or key). (SOURCE: CNSSI-4009)

A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g., in a public key certificate). (SOURCE: NIST SP 800-63)

Trusted Agent:
Entity authorized to act as a representative of an agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. (SOURCE: NIST SP 800-32; CNSSI-4009)

Trusted Computer System:
A system that employs sufficient hardware and software assurance measures to allow its use for processing simultaneously a range of sensitive or classified information. (SOURCE: CNSSI-4009)

Trustworthiness:
The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. (SOURCE: NIST SP 800-79; CNSSI-4009; NIST SP 800-39)

Security decisions with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities. (SOURCE: FIPS 201)

Tunneling:
Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. (SOURCE: CNSSI-4009)

Twitter:
An online social networking and microblogging service that enables users to send and read short 140-character text messages, called "tweets". Registered users can read and post tweets, but unregistered users can only read them. Users access Twitter through the website interface, SMS, or mobile device app. (SOURCE: Wikipedia)

Two Factor Authentication:
An approach that provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. (SOURCE: Wikipedia)

UNAUTHORIZED ACCESS – USER ID

Unauthorized Access:
Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. (SOURCE: FIPS 191)

Any access that violates the stated security policy. (SOURCE: CNSSI-4009)

Unauthorized Disclosure:
An event involving the exposure of information to entities not authorized access to the information. (SOURCE: NIST SP 800-57 Part 1; CNSSI-4009)

Uniform Resource Locator (URL):
A specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI. URLs are commonly used for web pages (http), but can also be used for file transfer (ftp), email (mailto) and many other applications. (SOURCE: Wikipedia)

Untrusted Process:
Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms. (SOURCE: CNSSI-4009)

User:
The term "user" refers to any Executive Branch agency full-time or part-time employee, temporary worker, volunteer, intern, contractor, and those employed by contracted entities, who are provided authorized access to State information assets.
(State of New Hampshire Statewide Information Security Manual)

Individual or (system) process authorized to access an information system. (SOURCE: FIPS 200)

Individual, or (system) process acting on behalf of an individual, authorized to access an information system. (SOURCE: NIST SP 800-53; NIST SP 800-18; CNSSI-4009)

An individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services. (SOURCE: FIPS 140-2)

User Datagram Protocol (UDP):
One of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths.
(SOURCE: Wikipedia)

User-ID:
Unique symbol or character string used by an information system to identify a specific user.
(SOURCE: CNSSI-4009)

VALIDATION – VULNERABILITY SCANNING

Validation:
The process of demonstrating that the system under consideration meets in all respects the specification of that system. (SOURCE: FIPS 201)

Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements). (SOURCE: CNSSI-4009)

Vendor:
A vendor, or a supplier, is a supply chain management term that means anyone who provides goods or services to a company or individuals. A vendor often manufactures inventoriable items and then sells those items to a customer. (SOURCE: Wikipedia)

Verification:
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). (SOURCE: CNSSI-4009)

Virtual LAN (VLAN):
In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN. (SOURCE: Wikipedia)

Virtual Machine (VM):
Software that allows a single host to run one or more guest operating systems.
(SOURCE: NIST SP 800-115)

Virtual Private Cloud (VPC):
An on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources. (SOURCE: Cloud Security Alliance)

Virtual Private Network (VPN):
VPNs extend a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and

management policies of the private network. A VPN is created by establishing a virtual point-to-point connection using dedicated connections, virtual tunneling protocols, or traffic encryptions. (SOURCE: Wikipedia)

Virtualization:
Refers to the logical abstraction of computing resources from physical constraints. One common abstraction is referred to as virtual machines or VMs, which takes the content of a physical machine and allows it to operate on different physical hardware and/or along with other virtual machines on the same physical hardware. In addition to VMs, virtualization can be performed on many other computing resources, including applications, desktops, networks, and storage.
(SOURCE: PCI DSS GLOSSARY)

The simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM). (SOURCE: NIST)

Virus:
A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. (SOURCE: CNSSI-4009)

Voice over IP (VoIP):
A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, IP communications, and broadband phone service. (SOURCE: Wikipedia)

Vulnerability:
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
(SOURCE: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-37; NIST SP 800-60; NIST SP 800-115; FIPS 200)

A weakness in a system, application, or network that is subject to exploitation or misuse.
(SOURCE: NIST SP 800-61)

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. (SOURCE: CNSSI-4009)

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

WARM SITE - ZEROIZATION

Warm Site:
An environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption. (SOURCE: NIST SP 800-34)

Backup site that typically contains the data links and preconfigured equipment necessary to rapidly start operations but does not contain live data. Thus, commencing operations at a warm site will (at a minimum) require the restoration of current data. (SOURCE: CNSSI-400)

Web-Based Connection:
The connection provides access to one or more applications through a single centralized interface, through a direct application access or portal architecture, typically a web-browser to a portal server located within the demilitarized zone (DMZ). This type of connection creates an area that serves as a boundary between two or more networks and isolates the information asset from the internal private network. (SOURCE: State of New Hampshire Statewide Information Security Manual)

Web Bug:
A tiny image, invisible to a user, placed on Web pages in such a way to enable third parties to track use of Web servers and collect information about the user, including IP address, host name, browser type and version, operating system name and version, and cookies. (SOURCE: NIST SP 800-28)

WiFi Protected Access (WPA):
Security protocol created to secure wireless networks. WPA is the successor to WEP. WPA2 was also released as the next generation of WPA. (SOURCE: PCI DSS GLOSSARY)

Wired Equivalent Privacy (WEP):
A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is no longer considered a viable encryption mechanism due to known weaknesses. (SOURCE: NIST SP 800-48)

Workaround:
Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available. (SOURCE: ITIL V3)

Worm:
A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See Malicious Code. (SOURCE: CNSSI-4009)

Zeroization:
A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. (SOURCE: FIPS 140-2)

A method of erasing electronically stored data, cryptographic keys, and Credentials Service Providers (CSPs) by altering or deleting the contents of the data storage to prevent recovery.