Glossary
Common Cybersecurity Terminology

Access
Ability to make use of any information system (IS) resource.

Source: CNSSI 4009-2015

Access control
The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Source: FIPS 201-2

Access control mechanism
Security safeguards designed to detect and deny unauthorized access and permit authorized access to an information system.

Source: CNSSI 4009-2015

Advanced Persistent Threat
An adversary that possesses sophisticated levels of expertise and significant resources which 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: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) 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 Rev. 1 (DHS Risk Lexicon)

Air gap
An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e. data is transferred through the interface only manually, under human control).

Source: CNSSI 4009-2015

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

Source: CNSSI 4009

Antivirus 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 800-94, NIST SP 800-83 Rev. 1

Asset
A major application, general support system, high impact program, physical plan, mission critical system, personnel, equipment, or a logically related group of systems.

Source: CNSSI 4009-2015

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

Source: NIST SP 800-82 Rev. 2 (CNSSI 4009)

Attack signature
A specific sequence of events indicative of an unauthorized access attempt.

Source: NIST SP 800-12

Attacker
A party who acts with malicious intent to compromise an information system.

Source: NIST SP 800- 63 Rev 2

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 (CNSSI 4009)

Audit Log

A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Source: NIST SP 800-53 Rev. 4

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Source: CNSSI 4009 (FIPS 200, NIST SP 800-27 Rev. A)

Authority

The aggregate of people, procedures, documentation, hardware, and/or software necessary to authorize and enable security-relevant functions.

Source: NIST SP 800-57 Part 2

Availability
Timely, reliable access to data and information services for authorized users.

Source: CNSSI 4009-2015, NIST SP 800-70 Rev 2

Backups
A copy of files and programs made to facilitate recovery if necessary.

Source: NIST SP 800-34 Rev. 1

Black-box testing
A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing.

Source: CNSSI 4009-2015, IST SP 800-53A Rev 4. (adapted)

Blacklist
A list of entities that are blocked or denied privileges or access.

Source: CNSSI 4009-2015 (NIST SP 800-94)

Breach
Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected information.

Source: ISO/IEC 27040

(adapted)

Common Vulnerabilities and Exposures (CVE)
A nomenclature and dictionary of security-related software flaws.

Source: CNSSI-4009-2015 (NIST SP 800-126 Rev. 2)

Compromise
A violation of the security policy of a system such that an unauthorized disclosure, modification, or destruction of sensitive information has occurred.

Source: CNSSI-4009-2015

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Source: CNSSI 4009-2015, NIST SP 800-39

Continuous Monitoring

Maintaining ongoing awareness to support organization risk decisions.

Source: CNSSI 4009-2015 (NIST SP 800-137)

Critical infrastructure

System and assets, whether physical or virtual, so vital to the United States 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.

Source(s): NIST SP 800-30

Critical infrastructure Sector

A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society.

Source: NIPP 2013 Partnering for Critical Infrastructure Security and Resilience

Cryptography

The use of mathematical techniques to provide security services such as confidentiality, data integrity, entity authentication, and data origin authentication.

Source: NIST SP 800-130

Cybersecurity

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: CNSSI 4009-2015 (NSPD-54/HSPD-23)

Data Loss

The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.

Source: CNSSI 4009-2015 (NIST SP 800-37)

Decipher

Convert enciphered text to plain text by means of a cryptographic system.

Source: CNSSI 4009-2015

Decryption

The process of changing ciphertext into plain text using a cryptographic algorithm and key.

Source: NIST SP 800-133

Denial of Service

The prevention of authorized access to resources or the delating of time-critical operations.

Source: NIST SP 800-33

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

The result of a cryptographic transformation of data which, when properly implemented, provides the services of: 1) origin authentication, 2) data integrity, and 3) signer non-repudiation.

Source: FIPS 140-2

Disruption

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 Rev. 1

Encrypt

Cryptographically transform data to produce cipher text.

Source: CNSSI 4009-2015

Encryption

The process of changing plain text into ciphertext for the purpose of security or privacy.

Source: NIST SP 800-21 Second Edition (NIST SP 800-57)

Endpoint Protection Platform

Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, antiadware, personal firewalls, host-based intrusion detection and prevention systems, etc.).

Source: NIST SP 800-128

Event

Any observable occurrence in a network or system.

Source: CNSSI 4009-2015 (NIST SP 800-61 Rev. 2)

Exfiltration

The unauthorized transfer of information from an information system.

Source: CNSSI 4009-2015 (NIST SP 800-53 Rev. 4)

Exploit

A technique to breach the security of a network or information system in violation of security policy.

Source: ISO/IEC 27039 (adapted)

Firewall

The process integrated with a computer operating system that detects and prevents undesirable applications and remote users from accessing or performing operations on a secure computer.

Source: NIST SP 800-130

Hack

Unauthorized attempt or access to an information system.

Source: CNSSI 4009-2015 (Adapted from "Hacker")

Hacker

Unauthorized user who attempts to or gains access to an information system.

Source: CNSSI 4009-2015

Hash Function

An algorithm that computes a numerical value (called the hash value) on a data file or electronic message that is used to represent that file or message, and depends on the entire contents of the file or message. A hash function can be considered to be a fingerprint of the file or message.

Source: NIST SP 800-152

Incident

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

Incident Handling

The mitigation of violations of security policies and recommended practices.

CNSSI 4009-2015, NIST SP 800-61 Rev. 2

Incident Response Plan

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 systems(s).

Source: CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)

Indicator

A sign that an incident may have occurred or may be currently occurring.

Source: NIST SP 800-61 Rev. 2

Information Operations (I/O)

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO.

Source: CNSSI 4009-2015

Information security policy

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Source: NIST SP 800-128 (CNSSI 4009)

Information system resilience

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

Source: CNSSI 4009-2015 (NIST SP 800-39)

Information technology

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes computers, ancillary equipment, software, firmware, similar procedures, services, and related resources.

Source: NIST SP 800-64 Rev. 2

Insider threat

An entity with authorized access (i.e., within the security) that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Source: NIST SP 800-53 Rev. 4 (CNSSI 4009)

Interoperability

A measure of the ability of one set of entities to physically connect to and logically communicate with another set of entities.

Source: NIST SP 800-130

Intrusion

A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so.

Source: CNSSI 4009-2015 (IETF RFC 4949 Ver 2)

Intrusion Detection and Prevention

The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents.

Source: NIST 800-94

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.

Source: NIST SP 800-111

Multifactor Authentication

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Source: NIST SP 800-53 Rev. 4

Non-repudiation

Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.

Source: NIST SP 800-32

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

Password

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

Source: FIPS 140-2

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

Penetration Testing

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

Phishing

Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Source: SP 800-45 Ver 2

Port

The entry or exit point from a computer for connecting communications or peripheral devices.

Source: NIST SP 800-82 Rev. 2

Port scanning

Using a program to remotely determine which ports on a system are open (e.g., whether the systems allow connections through those ports).

Source: NIST SP 800-82 Rev. 2 (NIST SP 800-61)

Private key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.

Source: FIPS 186-4

Probe

A technique that attempts to access a system to learn something about the system.

Source: CNSSI-4009

Public key

A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm and is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key.

Source: FIPS 186-4

Quarantine

To store files containing malware in isolation for future disinfection or examination.

Source: NIST SP 800-114

Resilience

The ability 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 800-137 (Adapted from NIST SP 800-39)

Risk analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

NIST SP 800-33

Risk assessment

The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

NIST SP 800-33

Scanning

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

Source: CNSSI 4009-2015

Spear Phishing

A colloquial term that can be used to describe any highly targeted phishing attack.

Source: CNSSI 4009-2015

Spoofing

Faking the sending address of a transmission to gain illegal entry into a secure system.

Source: CNSSI 4009-2015

Structured Query Language (SQL) injection

An attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code.

Source: US-CERT SQL Injection Publication

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 SP 800-161 (Adapted from ISO/IEC 15288, NIST SP 800-53 Rev. 4)

Supply Chain

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

Source: CNSSI 4009-2015

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: CNSSI 4009-2015 (NIST SP 800-27 Rev. A)

Tabletop Exercise

A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Source: NIST SP 800-84

Target of Attack

An information technology product or system and associated administrator and user guidance documentation that is the subject of an attack.

Source: FIPS 140-2 (Adapted from Target of Evaluation)

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: CNSSI 4009-2015 (NIST SP 800-31 Rev. 1)

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 4009-2015

Unauthorized access

Any access that violates the stated security policy.

Source: CNSSI 4009

Vulnerability

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

Source: FIPS 200 (Adapted from CNSSI 4009-2015)

Whitelist

A list of discrete entities, such as hosts, email addresses, network port numbers, runtime processes, or applications that are authorized to be present or active on a system according to a well-defined baseline.

Source: NIST SP 800-167