Term	NIST Definition	Definition Source
Account Management (User)	User account management involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.	NIST SP 800-12
Antivirus Software	A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.	• NIST SP 800-94 • NIST SP 800-83 Rev. 1
Application	The system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications.	NIST SP 800-16
Assessors	The individual responsible for conducting assessment activities under the guidance and direction of a Designated Authorizing Official. The Assessor is a 3rd party.	NIST SP 800-79-2
Assets	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.	CNSSI 4009-2015
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 (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.	NIST SP 800-27 Rev. A
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.	NIST SP 800-32 (CNSSI 4009)
Backup	A copy of files and programs made to facilitate recovery, if necessary.	CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)
Backup (system)	The process of copying information or processing status to a redundant system, service, device or medium that can provide the needed processing capability when needed.	NIST SP 800-152
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).	NIST SP 800-53 Rev. 4
Business Continuity Plans	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.	• NIST SP 800-34 Rev. 1 • CNSSI 4009-2015 (NIST SP 800-34 Rev. 1)
Certificate	A digital representation of information which at least 1) identifies the certification authority issuing it, 2) names or identifies its subscriber, 3) contains the subscriber's public key, 4) identifies its operational period, and 5) is digitally signed by the certification authority issuing it.	SP 800-32
Certificate Authority (CA)	A trusted entity that issues and revokes public key certificates.	NIST SP 800-63-2
Certificate Policy	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.	• CNSSI-4009 • SP 800-32
Cloud Infrastructure	The collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.	NIST SP 800-146
Code	A set of instructions for a computer.	CNSSI 4009-2015
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 cryptographic security, transmission security, emissions security, and physical security of COMSEC material.	CNSSI 4009-2015 (CNSSI 4005)

Term	NIST Definition	Definition Source
Compartmentalization	A nonhierarchical grouping of information used to control access to data more finely than with hierarchical security classification alone.	CNSSI 4009-2015
Compliance	Conformity in fulfilling official requirements.	NIST SP 800-146
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 (DRP) for major disruptions.	CNSSI 4009-2015
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.	• CNSSI 4009-2015 (NIST SP 800-37 Rev. 1, FIPS 200) • NIST SP 800-137 (CNSSI 4009) • NIST SP 800-18 Rev. 1 (CNSSI 4009) • NIST SP 800-37 Rev. 1 (CNSSI 4009) • NIST SP 800-53 Rev. 4 (CNSSI 4009)
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.	NIST SP 800-30
Cryptographic Security	Component of COMSEC that results from the provision of technically sound cryptographic systems and their proper use.	CNSSI 4009-2015 (NSA/CSS Manual Number 3-16 (COMSEC))
Demilitarized Zone	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) 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.	• NIST SP 800-82 Rev. 2 • CNSSI 4009-2015
Disaster Recovery Plan	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.	NIST SP 800-82 Rev. 2 (NIST SP 800-34)
E-authentication	The process of establishing confidence in user identities electronically presented to an information system.	• NIST SP 800-63-2 • CNSSI 4009-2015 (NIST SP 800-63-2)
Emissions Security (EMSEC)	The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptoequipment and information systems.	CNSSI 4009-2015 (JP 6-0)
End-Point 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.).	NIST SP 800-128
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.	• CNSSI 4009-2015 • NIST SP 800-30 (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.	CNSSI 4009-2015 (JP 6-0)
Exploitable Channel	Channel that allows the violation of the security policy governing an information system and is usable or detectable by subjects external to the trusted computing base.	CNSSI 4009-2015
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 in order to achieve a common level of quality or some level of interoperability.	NIST SP 800-161 (NIST SP 800-64 Rev. 2)
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.	NIST SP 800-47
Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.	CNSSI 4009-2015
Hacker	Unauthorized user who attempts to or gains access to an information system.	CNSSI 4009-2015
High Availability	A failover feature to ensure availability during device or component interruptions.	NIST SP 800-113

Term	NIST Definition	Definition Source
Homeland Security Presidential Directive 12 (HSPD-12)	HSPD-12 established the policy for which FIPS 201-2 was developed.	NIST SP 800-79-2
Identity	The set of physical and behavioral characteristics by which an individual is uniquely recognizable.	• FIPS 201-2 • NIST SP 800-79-2
Identity-Based Authentication	A process that provides assurance of an entity's identity by means of an authentication mechanism that verifies the identity of the entity. Contrast with role-based authentication.	NIST SP 800-152
Identity, Credential, and Access Management (ICAM)	Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (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.	CNSSI 4009-2015 (FICAM Roadmap and Implementation Guidance V2.0)
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.	• FIPS 200 • NIST SP 800-128 (FIPS 200) • NIST SP 800-137 (FIPS 200) • NIST SP 800-171 (Updates to version published June 2015) (FIPS 200) • NIST SP 800-53 Rev. 4 (FIPS 200) • NIST SP 800-82 Rev. 2 (FIPS 200, NIST SP 800-53)
Incident Handling	The mitigation of violations of security policies and recommended practices.	• CNSSI 4009-2015 • NIST SP 800-61 Rev. 2
Incident Response Plans	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).	• CNSSI 4009-2015 • NIST SP 800-34 Rev. 1
Information Assurance	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.	• NIST SP 800-161 (CNSSI 4009) • NIST SP 800-59 (CNSSI 4009)
Information Security Continuous Monitoring	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.].	NIST SP 800-137
Information System Contingency Management Plan	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.	NIST SP 800-34 Rev. 1
Inicident Handling	The mitigation of violations of security policies and recommended practices.	• CNSSI 4009-2015 • NIST SP 800-61 Rev. 2
Insider Threat	An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.	NIST SP 800-53 Rev. 4 (CNSSI 4009)
Interface	A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals.	FIPS 140-2
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.	CNSSI 4009-2015 (IETF RFC 4949 Ver 2)
Intrusion Detection	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.	• CNSSI 4009 • NIST SP 800-94
Intrusion 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.	• CNSSI 4009-2015 • NIST SP 800-94
Intrusion Prevention Systems	A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.	NIST SP 800-82 Rev. 2
Malware	A computer program that is covertly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or OS. Common types of malware threats include viruses, worms, malicious mobile code, Trojan horses, rootkits, and	NIST SP 800-114
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.	• CNSSI 4009-2015 (NIST SP 800-53 Rev. 4) • NIST SP 800-53 Rev. 4
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).	NIST SP 800-171 (Updates to version published June 2015)

Term	NIST Definition	Definition Source
Network Defense	Programs, activities, and the use of tools necessary to facilitate them (including those governed by NSPD-54/HSPD-23 and NSD-42) conducted on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting (1) that computer, network, or system; (2) data stored on, processed on, or transiting that computer, network, or system; or (3) physical and virtual infrastructure controlled by that computer, network, or system. Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners.	CNSSI 4009-2015 (PPD 20)
Network Intrusion Detection System	Software that performs packet sniffing and network traffic analysis to identify suspicious activity and record relevant information.	NIST SP 800-86
Network Mapping	A process that discovers, collects, and displays the physical and logical information required to produce a network map.	CNSSI 4009-2015 (CNSSI 1012)
Operations Security (OPSEC)	Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.	NIST SP 800-53 Rev. 4 (CNSSI 4009)
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.	SP 800-53A
Personal Identity Verification Card	A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).	FIPS 201-2
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.	• NIST SP 800-45 Version 2 • NIST SP 800-83 Rev. 1
Private Key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.	FIPS 201-2
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.	• NIST SP 800-32 • NIST SP 800-63-2
Remediation	The act of mitigating a vulnerability or a threat.	CNSSI 4009-2015 (Adapted from NIST SP 800-40 Rev. 2)
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	• NIST SP 800-137 (Adapted from FIPS 200) • NIST SP 800-30 (CNSSI 4009)
Risk Assessments	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.	CNSSI 4009-2015 (NIST SP 800-39)
Secuirty Audit	Independent review and examination of a system’s records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.	NIST SP 800-82 Rev. 2 (ISO/IEC 7498)
Secure State	Condition in which no subject can access any object in an unauthorized manner.	CNSSI 4009-2015
Security Control Automation Protocol (SCAP)	A suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. Note: There are six individual specifications incorporated into SCAP: CVE (common vulnerabilities and exposures); CCE (common configuration enumeration); CPE (common platform enumeration); CVSS (common vulnerability scoring system); OVAL (open vulnerability assessment language); and XCCDF (eXtensible configuration checklist description format).	CNSSI 4009-2015 (Adapted from NIST SP 800-126 Rev. 2)

Term	NIST Definition	Definition Source
Security Controls	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.	• NIST SP 800-161 (Adapted from FIPS 199) • NIST SP 800-171 (Updates to version published June 2015) • NIST SP 800-53 Rev. 4 (Adapted from FIPS 199)
Security Policy	The rules and requirements established by an organization that governs the acceptable use of its information and services, and the level and means for protecting the confidentiality, integrity, and availability of its information.	NIST SP 800-130
Service	A software component participating in a service-oriented architecture that provides functionality or participates in realizing one or more capabilities.	NIST SP 800-95 (Open Grid Services Architecture Glossary of Terms)
Situational Awareness	Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.	CNSSI 4009-2015
Spam Filtering Software	A program that analyzes e-mails to look for characteristics of spam, and typically places messages that appear to be spam in a separate e-mail folder.	NIST SP 800-69
Strong Authentication	A method used to secure computer systems and/or networks by verifying a user's identity by requiring two-factors in order to authenticate (something you know, something you are, or something you have).	CNSSI 4009-2015 (DoDI 8420.01)
Threats	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.	FIPS 200 (Adapted from CNSSI 4009)
Token Authenticator	The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it.	NIST SP 800-63-2
Transmission Security (TRANSEC)	Measures (security controls) applied to transmissions in order 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 which deals with the security of communication transmissions, rather than that of the information being communicated.	CNSSI 4009-2015
Trust	A characteristic of an entity that indicates its ability to perform certain functions or services correctly, fairly, and impartially, along with assurance that the entity and its identifier are genuine.	NIST SP 800-130
Validation	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).	CNSSI 4009-2015
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.	• CNSSI 4009-2015 • NIST SP 800-161 • NIST SP 800-39 • NIST SP 800-53 Rev. 4 • NIST SP 800-30
Vulnerability Scanning	A technique used to identify hosts/host attributes and associated vulnerabilities.	NIST SP 800-115
X.509 Certificate	Public key certificates that contain three nested elements: 1) the tamper-evident envelope (digitally signed by the source), 2) the basic certificate content (e.g., identifying information and public key), and 3) extensions that contain optional certificate information.	NIST SP 800-57 Part 2