# Cybersecurity Terms and Definitions for Acquisition

| Terms | NIST Definition | Definition Source |
|---|---|---|
| Account Management (User) | User account management involves<br>(1) the process of requesting, establishing, issuing, and closing user accounts;<br>(2) tracking users and their respective access authorizations; and<br>(3) managing these functions. | NIST SP  800-12 Rev. 1 |
| 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 800-83 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 |
| Assessment and Authorization (A&A) | Assessment is the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meet a set of specified security requirements. Authorization is a formal declaration by the Authorizing Official (AO) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk to the agency. | NIST Special Publication 800-53 (Rev. 4) |
| Assessor | The individual responsible for conducting assessment activities under the guidance and direction of a Designated Authorizing Official. The Assessor is a third party. | NIST SP 800-79-2 |
| Assets | Resources of value that an organization possesses or employs. | NISTIR 8011 Vol. 1 under Asset |
| 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 800-12 Rev. 1 under Assurance |
| 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. | NIST SP 800-12 Rev. 1 under Audit |
| Backup | A copy of files and programs made to facilitate recovery, if necessary. | NISTIR 7621 Rev. 1 under Backup (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 |
| Best in Class (BIC) | BIC means that something has been designated by the Office of Management and Budget (OMB) as a preferred government-wide solution that:<br>1) Allows acquisition experts to take advantage of pre-vetted, government-wide contract solutions;<br>2) Supports a government-wide migration to solutions that are mature and market-proven;<br>3) Assists in the optimization of spend, within the government-wide category management framework; and<br>4) Increases the transactional data available for agency level and government-wide analysis of buying behavior. | Best-In-Class GSA web page |
| 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). | CNSSI 4009-2015 (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 under Business Continuity Plan (BCP)<br>• CNSSI 4009-2015 (NIST SP 800-34 Rev. 1) |
| Certificate | A digital representation of information which at least:<br>1) identifies the certification authority issuing it,<br>2) names or identifies its subscriber,<br>3) contains the subscriber's public key,<br>4) identifies its operational period, and<br>5) is digitally signed by the certification authority issuing it. | CNSSI 4009-2015 (NIST SP 800-32 - CNSSI No. 1300 ) |
| Certificate Authority (CA) | A trusted entity that issues and revokes public key certificates. | NISTIR 8149 |
| 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 4009-2015 (NIST SP 800-32) |
| Certification And Accreditation (C&A) | 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. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. This process is now called Assessment and Authorization (see definition above) to follow the language of the Risk Management Framework. This is the previous industry term for A&A. | NIST SP 800-64 Rev. 2 (NIST SP 800-37) |

| Terms | NIST Definition | Definition Source |
|---|---|---|
| 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 800-145 |
| Code | System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. | CNSSI 4009-2015 (NSTISSI No. 7002) |
| Commercial Supplier Agreement (CSA) | GSA's CSAs define the terms and conditions for selling technology products through GSA Multi-Award Schedules. Before DHS reviews products for potential inclusion in the Continuous Diagnostics and Mitigation Approved Product List, a vendor must have a CSA in place with GSA. | GSA.gov |
| 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) |
| Compartmentalization | A non-hierarchical 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 |
| 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. | CNSSI 4009-2015 |
| Configuration Management | A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. | NIST SP 800-171 Rev. 1 |
| Configuration Settings | The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the system. | NIST SP 800-171 Rev. 1 |
| Contingency Plan | A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. | NIST SP 800-57 Part 1 Rev. 4 under Contingency plan |
| Continuous Diagnostics and Mitigation (CDM) | The CDM program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. | Continuous Diagnostics & Mitigation (CDM) Program webpage on GSA.gov |
| Continuous Monitoring | Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. | NIST SP 800-150 under Continuous Monitoring (NIST SP 800-137) |
| Continuity of Operations Plan (COOP) | An effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions (PMEFs) continue to be performed during a wide range of emergencies, including localized acts of nature, accidents and technological or attack-related emergencies. | National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive51/Homeland Security Presidential Directive20 (NSPD-51/HSPD-20) / CNSSI 4009-2015 (NIST SP 800-34 Rev. 1) |
| Countermeasures | The 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. | CNSSI 4009-2015 under safeguards (FIPS 200) |
| Database | A repository of information that usually holds plant-wide information including process data, recipes, personnel data, and financial data. | NIST SP 800-82 Rev. 2 (NISTIR 6859) |
| Database Assessment | Assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities. | HACS RFQ Template |
| Defense-In-Depth | The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. | NISTIR 8183 under Defense-in-depth (ISA/IEC 62443) |
| 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<br>• CNSSI 4009-2015 |
| DHS CDM APL (CDM Approved Products List) | The hardware and software products and associated services under the Continuous Diagnostics & Mitigation Tools SIN. These products undergo a product qualification process by Department of Homeland Security in order to be added to the list. | Continuous Diagnostics & Mitigation (CDM) Program webpage |
| 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 presented digitally to a system. | NIST SP 800-63-3 under Digital Authentication |
| eBuy | An electronic Request for Quote (RFQ) / Request for Proposal (RFP) system designed to allow government buyers to request information, find sources, and prepare RFQs/RFPs, online, for millions of services and products offered through GSA's Multiple Award Schedule and GSA Technology Contracts. eBuy Open is only available to Federal government users registered on the Acquisition Gateway. | www.ebuy.gsa.gov Home Page |

| Terms | NIST Definition | Definition Source |
|---|---|---|
| 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 crypto-equipment and information systems. | CNSSI 4009-2015 (JP 6-0) |
| eMod | A web-based application that allows Multiple Award Schedule contractors to electronically prepare and submit contract modifications to Federal Acquisition Services. | www.eoffer.gsa.gov ABOUT EMOD webpage |
| End-Point Protection Platform | Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, anti-spyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.). | NIST SP 800-128 |
| End-User License Agreement (EULA) | A EULA is a legal contract between a user and the software publisher. It spells out the terms and conditions for using the software. A user can refuse to accept the terms and conditions of the EULA, but then they cannot legally use the software. | https://www.US-Cert.gov |
| 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<br>• 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 | A 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 |
| External Security Testing | Security testing conducted from outside the organization's security perimeter. | NIST SP 800-115 |
| 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. | CNSSI 4009-2015<br>NIST SP 800-53 Rev. 4 |
| 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 800-63-3 / NIST SP 800-161 (NIST SP 800-64 Rev. 2) |
| Federal Information Security Modernization Act (FISMA) | The Federal Information Security Modernization Act (FISMA) requires agencies to integrate IT security into their capital planning and enterprise architecture processes at the agency, conduct annual IT security reviews of all programs and systems, and report the results of those reviews to the Office of Management and Budget (OMB). | NIST |
| Firewall | A part of a computer system or network that is designed to block unauthorized access while permitting outward communication. | NIST SP 800-152 under Firewall |
| 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 |
| Government-wide Acquisition Contracts (GWACs) | GWACs provide access to IT solutions such as systems design, software engineering, information assurance, and enterprise architecture solutions. Small business set-aside GWACs also provide socioeconomic credit. More information about GSA Government-wide Acquisition Contracts (GWACs) can be found at www.gsa.gov/gwacs. | Data To Decision Customer GSA web page |
| Government-wide Acquisition Contract (GWAC) Prices Paid Suite | The GWAC Prices Paid Suite of tools provide customer agencies with data that will aid in conducting (a) realistic price analysis; (b) negotiations; (c) independent government cost estimates (IGCE); and (d) aid in benchmarking competitive pricing.<br>The GWAC Prices Paid Suite of tools provide agencies with price range (low, average, & high) for each functional labor category on the Alliant and Alliant Small Business GWAC by using the Life of Contract Analysis Dashboard and the Labor Analysis Dashboard, both of which can aid federal agency users in price analysis and negotiations.<br>Agency users can conduct improved market research and develop more realistic independent government cost estimates (IGCE) by using the Labor Analysis Dashboard. These provide customers a more detailed view of the prices paid on labor categories for Time and Material (T&M) and Labor Hour (LH) contract types. | Data To Decision Customer GSA web page |
| GSA Advantage! | An online shopping and ordering system that provides access to thousands of contractors and millions of supplies (products) and services. Anyone may browse on GSA Advantage!® to view and compare the variety of products and services offered. HACS and CDM Tools can be purchased on GSA Advantage. | GSA Advantage! web page on GSA.gov |
| 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 |
| Highly Adaptive Cybersecurity Services (HACS) | Pre-vetted support services that will expand agencies' capacity to test their high-priority IT systems, rapidly address potential vulnerabilities, and stop adversaries before they impact their networks. | Highly Adaptive Cybersecurity Services (HACS) GSA web page |

| Terms | NIST Definition | Definition Source |
|---|---|---|
| High Value Asset (HVA) | Assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people.<br>They may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S Government. | OMB Memo M-17-09 |
| 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 | An attribute or set of attributes that uniquely describe a subject within a given context. | NIST SP 800-63-3 under Identity |
| 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<br>• NIST SP 800-128 (FIPS 200)<br>• NIST SP 800-137 (FIPS 200)<br>• NIST SP 800-171 (Updates to version published June 2015) (FIPS 200)<br>• NIST SP 800-53 Rev. 4 (FIPS 200)<br>• 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<br>• NIST SP 800-61 Rev. 2 |
| Incident Response | Services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. | Highly Adaptive Cybersecurity Services (HACS) GSA web page |
| 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<br>• 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 800-12 Rev. 1 under Information Assurance (CNSSI 4009) |
| Information Security Continuous Monitoring (ISCM) | Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.<br>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 (ISCP) | 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 |
| Information Technology Infrastructure Library (ITIL), v3 | The organizational structure and skill requirements of an information technology organization and a set of standard operational management procedures and practices to allow the organization to manage an IT operation and associated infrastructure. The operational procedures and practices are supplier independent and apply to all aspects within the IT Infrastructure. | https://www.itlibrary.org/ |
| Information Technology (IT) Schedule 70 | Delivers federal, state, and local customer agencies the tools and expertise needed to shorten procurement cycles, ensure compliance, and obtain the best value for innovative technology products, services, and solutions.<br>With more than 7.5 million products and services from over 4,600 pre-vetted vendors, federal agencies, as well as civilian, state, and local organizations, continue to maximize budgets, and reduce buying cycles by up to 50 percent over open market. | GSA Schedule Web Page on GSA.gov |
| Infrastructure as a Service (IaaS) | The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). | Source(s): NIST SP 800-145 |
| Insider Threat | The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. | CNSSI 4009-2015 (CNSSD No. 504 - Adapted)<br>NIST SP 800-171 Rev. 1 |
| Interface | A logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals. | NIST SP 800-171 Rev. 1 |
| Internal Security Testing | Security testing conducted from inside the organization's security perimeter. | NIST SP 800-115 |

| Terms | NIST Definition | Definition Source |
|---|---|---|
| Internet Protocol Version 6 (IPv6) | IPv6 is the protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. | CNSSI 4009-2015 |
| 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<br>• 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<br>• NIST SP 800-94 |
| Intrusion Prevention Systems (IPS) | 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 |
| Least Privilege | 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. | CNSSI 4009-2015<br>NIST SP 800-171 Rev. 1 / NIST SP 800-12 Rev. 1 under Least Privilege (CNSSI 4009) |
| Malware | 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. | NIST SP 800-53 Rev. 4 under Malicious Code<br>CNSSI 4009-2015 under malicious code (NIST SP 800-53 Rev. 4)<br>NISTIR 7621 Rev. 1 under Malware (NIST SP 800-53 Rev. 4 - "Malicious Code") |
| 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)<br>• NIST SP 800-53 Rev. 4 |
| Memorandum of Understanding or Agreement (MOU) | A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes specific terms that are agreed to, and a commitment by at least one party to engage in action. It includes either a commitment of resources or binds a party to a specific action. | CNSSI 4009-2015 under memorandum of agreement (MOA) (DoDI 4000.19) |
| Multi-Factor Authentication (MFA) | 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 Rev. 1 under multifactor authentication |
| 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) |
| Operating System Security Assessment (OSSA) | The Operating System Security Assessment (OSSA) service assesses the configuration of select host operating systems (OS) against standardized configuration baselines (Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baselines (USGCB)). The results identify deviations from Government required baselines and recommended remediation steps to bring configurations into compliance. All assessment activities are conducted onsite at the stakeholder's location. Administrator or root-level access will be required for this service. | Highly Adaptive Cybersecurity Services (HACS) GSA web page |
| 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 (PIV) 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). | NIST SP 800-79-2 |
| Phishing | Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. | • CNSSI 4009-2015 (IETF RFC 4949 Ver 2)<br>• NIST SP 800-12 Rev. 1 under Phishing (IETF RFC 4949 Ver 2) |
| Platform as a Service (PaaS) | The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. | NIST SP 800-145 |

| Terms | NIST Definition | Definition Source |
|---|---|---|
| Private Key | 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 has a corresponding public key. Depending on the algorithm, the private key may be used, for example, to: 1. Compute the corresponding public key, 2. Compute a digital signature that may be verified by the corresponding public key, 3. Decrypt keys that were encrypted by the corresponding public key, or 4. Compute a shared secret during a key-agreement transaction. | NIST SP 800-57 Part 1 Rev. 4 under Private key |
| Public Key Infrastructure (PKI) | 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. | NIST SP 800-53 Rev. 4 under Public Key Infrastructure (CNSSI 4009) |
| Remediation | The act of mitigating a vulnerability or a threat. | CNSSI 4009-2015 (Adapted from NIST SP 800-40 Rev. 2) |
| Request for Quotation (RFQ) | A procurement solicitation in which an organization asks vendors to submit a quote for specific products and services. | eBuy GSA web page |
| 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)<br>• NIST SP 800-30 (CNSSI 4009) |
| Risk and Vulnerability Assessment | Assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. | Highly Adaptive Cybersecurity Services (HACS) GSA web page |
| 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) / NIST SP 800-53 Rev. 4 under Risk Assessment |
| Risk Management Framework (RMF) | Presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. | NIST SP 800-82 Rev. 2 under Risk Management Framework (NIST SP 800-37) |
| Rules of Engagement (ROE) | Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions. | NIST SP 800-115 |
| Security Architecture Review (SAR) | Evaluates a subset of the agency's high value asset (HVA) security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. It's process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. It provides a holistic analysis of how an HVA's individual security components integrate and operate, including how data is protected during operations. | 132-45 HACS SIN Terms & Conditions FAQ Document |
| Security 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) |
| 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.<br>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) / NIST SP 800-126 Rev. 3 under Security Content Automation Protocol (SCAP) |
| 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)<br>• NIST SP 800-171 Rev. 1 (FIPS 199 - Adapted) (Updates to version published June 2015)<br>• NIST SP 800-53 Rev. 4 (Adapted from FIPS 199) |
| Security Operations Center (SOC) | A facility where security information is housed, monitored and analyzed to protect data from cybersecurity threats. As security operations have evolved, and technology (including cloud) has advanced, more agencies are outsourcing their security capabilities. The result is SOCs may no longer consist of an onsite, dedicated team providing continuous support. | GSA.gov blog: A Federal Perspective on Security Operations Centers as a Service (SOCaaS) |
| Secure State | Condition in which no subject can access any object in an unauthorized manner. | CNSSI 4009-2015 |
| 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) |
| Simplified Acquisition Threshold (SAT) | The SAT identifies the maximum dollar value for an acquisition that can use the simplified acquisition procedures, which are used to reduce administrative costs and promote efficiency and economy in contracting. | CDM Tools SIN Ordering Procedure Document |

| Terms | NIST Definition | Definition Source |
|---|---|---|
| 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 |
| Social Engineering | The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust. | NIST SP 800-63-3 |
| Software as a Service (SaaS) | The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. | NIST SP 800-145 |
| Spam Filtering Software | A program that analyzes emails to look for characteristics of spam, and typically places messages that appear to be spam in a separate email folder. | NIST SP 800-69 |
| Special Item Numbers (SINs) | Alpha-Numeric values assigned to supplies and services which are categorized in each Schedule. It is a categorization method that groups similar products, services, and solutions together to aid in the acquisition process | List of Schedules GSA web page |
| Statement of Work (SOW) | An SOW describes the terms and objectives of a project or service contract, and includes the scope of work required to meet the objectives, costs, deliverables, timeliness, and other expectations. GSA.gov has a dedicated webpage with samples of technology SOWs. | Sample Technology Statements of Work web page |
| 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) |
| Systems Security Engineering (SSE) | A specialty engineering field strongly related to systems engineering. It applies scientific, engineering, and information assurance principles to deliver trustworthy systems that satisfy stakeholder requirements within their established risk tolerance. | CNSSI 4009-2015 (NIST SP 800-160 - (draft)) |
| Technical Surveillance Countermeasure Reviews (TSCM) | Techniques to detect, neutralize, and exploit technical surveillance technologies and hazards that permit the unauthorized access to or removal of information. | CNSSI 4009-2015 (DoDI 5240.05) |
| 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 800-63-3 |
| Transient Electromagnetic Pulse Emanation Standard (TEMPEST) | A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment. | CNSSI 4009-2015 (FIPS 140-2) |
| Transmission Control Protocol (TCP) | TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. | NIST SP 800-82 Rev. 2 (API 1164) |
| 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.<br>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 | An ISCM capability that ensures that untrustworthy persons are prevented from being trusted with network access (to prevent insider attacks). | NISTIR 8011 Vol. 1 under Capability, Trust Management |
| Trustworthy Information System | An information system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation. | OMB Memo M-19-03 / Circular A-130 |