Cybersecurity Terms and Definitions for Acquisition

Terms	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.	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12 Rev. 1
Advanced Persisent Threat (APT)	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.	NIST SP 800-30 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
Application Security Testing (AST)	Testing, analyzing, and reporting the security level of an application as it moves from early development stages through deployment and maintenance.An effective AST program incorporates products, services, and solutions that continuously assess and address application vulnerabilities through the entire software development life cycle.	GSA AST Webpage
Artificial Intelligence (AI)	a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.	House of Representatives (H.R.) 6216 - National Artificial Intelligence Initiative Act of 2020
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 SP 800-53 Rev. 5
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.	NIST Interagency or Internal Report (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

Terms	Definition	Definition Source
Backup	A copy of files and programs made to facilitate recovery, if necessary.	NISTIR 7621 Rev. 1 under Backup
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: 1) allows acquisition experts to take advantage of pre-vetted, government-wide contract solutions; 2) supports a government-wide migration to solutions that are mature and market-proven; 3) assists in the optimization of spend, within the government-wide category management framework; and 4) increases the transactional data available for agency level and government-wide analysis of buying behavior.	GSA Best-in-Class Technology Solutions
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. 5
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.	Committee on National Security Systems Instruction (CNSSI) 4009-2015
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.	CNSSI 4009-2015
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
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

Terms	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
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
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. 5 under Contingency plan
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.	CNSSI 4009-2015
Continuous Diagnostics and Mitigation (CDM) Program	The CDM Program provides a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program delivers cybersecurity tools, integration services, and dashboards that help participating agencies improve their security posture	CISA CDM Program webpage
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.	NIST SP 800-150 under Continuous Monitoring
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
Cryptographic Key Management	The framework and services that provide for the generation, production, establishment, control, accounting, and destruction of cryptographic keys.	NIST SP 800-57 Part 2 Rev. 1
Cybersecurity Supply Chain Risk Management (C-SCRM)	A systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures.	NIST SP 800-161r1
Data Loss Prevention (DLP)	Strategies and tools to prevent data breaches and unauthorized data transfer.	NIST SP 800-53 Rev. 5

Terms	Definition	Definition Source
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
Database Assessment	Assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.	NIST SP 800-115
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
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.	CNSSI 4009-2015
DHS CDM Approved Products List (APL)	The authoritative catalog for approved products that meet CDM technical requirements. Software and hardware manufacturers and resellers can submit products for APL consideration monthly. CISA reviews each submission against established CDM Program criteria to validate the vendor's claim that each product meets the requirements for the capability category for which it was submitted. The CDM APL is managed by the CISA Cybersecurity Division's Capacity Building Acquisition and Budget office.	CISA CDM APL 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
Dynamic AST (DAST) Tools	Analyze applications in their dynamic, running state during testing or operational phases. They simulate attacks against an application (typically webenabled applications, services, and APIs), analyze the application's reactions, and determine whether it is vulnerable.The dynamic aspect helps the system catch dependencies that are being loaded at launch time, such as those that would not be caught by Static AST tools.	NIST SP 800-204C
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.	GSA eBuy website
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
eMod	A web-based application that allows Multiple Award Schedule (MAS) contractors to electronically prepare and submit contract modifications to Federal Acquisition Services.	GSA eOffer webpage
Endpoint Detection and Response (EDR)	Endpoint Detection and Response performs behavioral analytics on endpoint events from Symantec Endpoint Protection to identify potentially malicious behavior.	NIST SP 1800-24
Endpoint 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.	GSA Article: GSA Publishes New Final Rule Addressing Commercial Supplier Agreement (CSA) Term

Terms	Definition	Definition Source
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.	NIST SP 800-30
Enterprise Infrastructure Solutions (EIS)	EIS is a comprehensive solution-based vehicle to address all aspects of federal agency IT, telecommunications, and infrastructure needs.	GSA EIS Webpage
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
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.	NIST SP 800-53 Rev. 5
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
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 FISMA webpage
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.	GSA GWACS webpage
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. 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. 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.	GSA Data To Decision Customer webpage

Terms	Definition	Definition Source
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! webpage
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
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. 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
Highly Adaptive Cybersecurity Services (HACS)	Evaluated proactive and reactive support services that can test high-priority IT systems, quickly order and implement services from technically-evaluated vendors, stop adversaries before they impact networks, and rapidly address potential vulnerabilities.	GSA HACS webpage
Homeland Security Presidential Directive 12 (HSPD-12)	HSPD-12 established the policy for which FIPS 201-2 was developed. For more information, visit: https://www.dhs.gov/homeland-security-presidential-directive-12	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
Identity and Access Management (IAM)	Broadly refers to the administration of individual identities within a system, such as a company, a network or even a country. In enterprise IT, identity management is about establishing and managing the roles and access privileges of individual network users.	NIST SP 800-175
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.	NIST SP 800-53 Rev. 5
Incident Handling	The mitigation of violations of security policies and recommended practices.	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.The mitigation of violations of security policies and recommended practices.	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).	NIST SP 800-61 Rev. 2
Information and Communications Technology (ICT)	Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information.	NIST SP 800-161r1

Terms	Definition	Definition Source
ICT Supply Chain	Linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling, and delivery of ICT products and services to the acquirer.	NISTIR 7622
ICT Supply Chain Risk	Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.	NISTIR 7622
ICT Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.	NISTIR 7622
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.	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 Category under the Multiple Award Schedule (MAS) Consolidated Solicitation (ITC-MAS)	A full suite of IT and telecommunications products, services, and solutions from highly qualified industry partners. Pre-competed contracts enable federal, state, and local customer agencies faster acquisition, federal acquisition regulation compliance, and lower prices.	GSA ITC Webpage
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.	The Information Technology Infrastructure Library webpage
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).	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.	NIST SP 800-171 Rev. 1
Interactive AST (IAST) Tools	Combine elements of Dynamic AST tools with the instrumentation of the application under test. They are typically implemented as an agent within the test runtime environment (e.g., instrumenting the Java Virtual Machine or .NET CLR) that observes operations or identifies and attacks vulnerabilities.	NIST SP 800-204C
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
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

Terms	Definition	Definition Source
Intrusion Detection	The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents.	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.	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
IT Asset Management (ITAM)	Management tool which helps to record and track the extent to which various assets contribute to the enterprise's mission.	NISTIR 8286A
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.	NIST SP 800-12 Rev. 1 under Least Privilege
Machine Learning (ML)	An application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.	H.R. 6216 - National Artificial Intelligence Initiative Act of 2020
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. 5
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.	NIST SP 800-53 Rev. 5
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)
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 Multi-Factor 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
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
Network Operations Center (NOC)	A network operations center (NOC) is a centralized location where computer, telecommunications, or satellite networks systems are monitored and managed 24x7. It is the first line of defense against network disruptions and failures.	IBM Topics website
NIST Cybersecurity Framework	A policy framework of computer security guidance for private sector organizations.	NIST Cybersecurity Framework (CSF) 2.0

Terms	Definition	Definition Source
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.	GSA HACS webpage
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. 5
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.	NIST 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.	NIST SP 800-12 Rev. 1 under Phishing
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
Post Quantum Cryptography (PQC)	An area of cryptography that researches and advances the use of quantum-resistant primitives, with the goal of keeping existing public key infrastructure intact in a future era of quantum computing. Intended to be secure against both quantum and classical computers and deployable without drastic changes to existing communication protocols and networks.	NIST Projects & Programs Post-Quantum Cryptography
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 800-53 Rev. 5
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. 5 under Public Key Infrastructure

Terms	Definition	Definition Source
Quantum and Information Science and Technology (QIST)	The merger of quantum physics and information theory. Quantum physics describes nature at an atomic and subatomic level. Information theory is the study of quantification, storage, and communication of information. Early examples of quantum technologies are lasers, transistors, magnetic resonance spectroscopy, and atomic clocks. These, in turn, gave us computers, the internet, medical imaging, and GPS navigation. Future technologies such as quantum computers, quantum networks, and quantum sensors are being researched and developed by combining quantum physics and information theory.	National Archives Quantum Information Science and Technology Implications for Records Management White Paper
Remediation	The act of mitigating a vulnerability or a threat.	CNSSI 4009-2015
Request for Quotation (RFQ)	A procurement solicitation tool in which an organization asks vendors to submit a quote for specific products and services.	Buy GSA webpage
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 800-30 (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.	GSA HACS webpage
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.	NIST SP 800-53 Rev. 5 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
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
Secure State	Condition in which no subject can access any object in an unauthorized manner.	CNSSI 4009-2015
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.	HACS Services Buyer's Guide
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
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).	NIST SP 800-126 Rev. 3 under Security Content Automation Protocol (SCAP)

Terms	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 800-53 Rev. 5
Security Information and Event Management (SIEM)	Tools and services that provide real-time analysis of security alerts generated by network hardware and applications.	NIST SP 800-92
Security Operations Center (SOC)	A security operations center (SOC) is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner.	NIST SP 800-53 Rev. 5
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
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.	HACS Services Buyer's Guide
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
Software Composition Analysis (SCA) Tools	Used to identify open-source and third-party components in use in an application, their known security vulnerabilities, and typically adversarial license restrictions.	NIST SP 800-204C
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.	GSA List of Schedules
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.	GSA Sample Technology Statements of Work webpage
Static AST (SAST) Tools	Analyze an application's source, bytecode, or binary code for security vulnerabilities, typically at the programming and/or testing software life cycle (SLC) phases. Involves techniques that look through the application in a commit and analyze its dependencies. If any dependencies contain issues or known security vulnerabilities, a commit will be marked as insecure and will not be allowed to proceed to deployment. This can also include finding hardcoded passwords / secrets in code that should be removed.	NIST SP 800-204C
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

Terms	Definition	Definition Source
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
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
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
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
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
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	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
Trusted Internet Connections (TIC)	A program to optimize and standardize the security of federal agencies' external network connections.	CISA TIC Core Guidance Volume 2: Reference Architecture
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
Vulnerability Management	The process of identifying, classifying, prioritizing, and mitigating software vulnerabilities.	NIST SP 800-40r4
Zero Trust	A collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.	NIST SP 800-207
Zero Trust Architecture (ZTA)	A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.	NIST SP 800-160 Vol. 2 Rev. 1