Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Accountability	The property that ensures that the actions of an entity may be traced uniquely to the entity.	ISO/IEC 7498-2	Being able to associate actors with their acts.	Pertains to the ability to record and track, with attribution of responsibility, the actions of users (whether humans or processes) while they are interacting with the software. This tracking must be possible both during and after the recorded interactions. [FIBS PUB 200, Minimum Security Requirements for Federal Information Systems]			Process of tracing IS activities to a responsible source.		The property that ensures that the actions of an entity may be traced uniquely to the entity [ISO/IEC 7498-2].
Adware	Software whose primary function is generating revenue by advertising targeted at the user of the computer on which the software resides.	McAfee	Any program that produces advertising while it executes. Many adware applications also track user information.	Any program that displays advertising.					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Anomaly	Anything observed in the documentation or operation of software that deviates from expectations based on previously verified software products or reference documents.	IEEE 610.12-1990						Anything observed in the documentation or operation of software that deviates from expectations based on previously verified software products or reference documents.	
Anonymity	Involves concealing one's identity, activities, attributes, relationships, and possibly existence.	DHS	Anonymity can involve concealing one's identity, activities, attributes, relationships, and possibly existence.						
Asset	Anything that has value (e.g., data, executing process) to a stakeholder (e.g., organization who owns it).	Modified ISO/IEC13335-2:2004	Anything of value to a stakeholder, particularly to its owner or attacker, but also to society or to the entity about whom data may relate. Secure software developers must identify assets and their protection needs.		A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems. Source: SP 800-26				Anything that has value to the organization [ISO/IEC 13335-2:2004]

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Assurance	Grounds for confidence that an entity meets its security objectives.	ISO/IEC 15408-1: 2005-10-01			Assurance- One of the five "Security Goals." Involves support for our confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. Source: SP 800-27A	Those activities, regardless of the organization conducting the activities, that demonstrate the conformance of a product or process to a specified criteria.	Measures of confidence that the security features, practices, procedures, and architecture of an IS accurately mediates and enforces the security policy.		Grounds for confidence that an entity meets its security objectives. ISO/IEC 15408-1: 2005-10-01

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Assurance Case	A reasoned, auditable argument created to support claims that the defined software intensive system will have grounds for confidence to satisfy requirements.	Modified Ministry of Defence. Defence Standard 00-42 Issue 2, Reliability and Maintainability (R&M) Assurance Guidance Part 3 R&M Case, 6 June 2003.	A reasoned, auditable argument created to support the contention that the defined software intensive system will satisfy software security requirements and objectives. UK Ministry of Defence Standard 000-42 [Ministry of Defence 2003b, section 4.1] Sometimes called an "assurance argument;" in this report the term "assurance argument" or just "argument" is used for the arguments that connect the evidence to the assurance conclusions.						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Authentication	The verification of identity of an entity.	CAS, Sam Redwine	A mechanism that firmly establishes identity.		Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. Source: SP 800-53		Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.		The provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication).ISO/IEC 18028-4: 2005-04-01
Autorooter	Scripts or programs for trying to obtain complete administrative privileges.								

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Availability	The property of being accessible and usable upon demand with acceptable response times by an authorized entity.	ISO/IEC 13335-1:2004	Readiness for service. May include availability to share.	SDLC - Software must continue to operate correctly and be accessible to its intended users{ FIPS Pub 200, Minimum Security Requirement for Federal Information Systems.}	Ensuring timely and reliable access to and use of information. Source: SP 800-53. A loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., SEC. 3542]		Timely, reliable access to data and information services for authorized users.	The degree to which a system or component is operational and accessible when required for use. Often expressed as a probability.	The property of being accessible and usable upon demand by an authorized entity. [ISO/IEC 13335-1:2004]

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Backdoor	Surreptitious mechanism used to circumvent security controls and provide access. Synonymous with trap door.	CNSSI 4009	Provides remote access to a system through a back door or open port. Synonymous with trap door.	Is malicious code that has the specific objective of enabling the attacker (or the web service that acts as a proxy service on the attacker's behalf) to bypass the targeted web service's (and/or its host's) authentication mechanisms to gain access to sensitive data or resources, without being detected; Undocumented command or features that allow knowledgeable perpetrators to access the web service host.			Hidden software or hardware mechanism used to circumvent security controls. Synonymous with trap door.		
Brute Force Attack	Attacking a system through repeated executions of similar actions.	CAS, Sam Redwine							Attack on a cryptosystem that employs an exhaustive search of a set of keys, passwords or other data.

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Buffer Overflow	An action where more input can be placed into a buffer or data holding area than the capacity allocated. Synonymous with buffer overrun.	Modified NIST	One of the most common vulnerabilities in software [Viega and McGraw 2002]. Occurs when a program reads or writes outside the bounds of a storage buffer.	Buffer overflows result when a program doesn't do bounds checking, and the input is accepted by the program and overflows the stack buffer that receives it.	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.				
Buffer Overrun	See buffer overflow.								
Commercial Off the Shelf (COTS)	*S*oftware or hardware products, which are ready-made and available for sale to the general public.	CAS				COTS software refers to purchased software such as operating systems, or application.	COTS software is widely available and developed with general commercial applications in mind. Such software typically has little or no U.S. Government funding or influence. NSTISSP 11		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO/IEC 13335-1:2004	The absence of authorized disclosure of information.	Software itself, rather than the data it accesses (or enables access to), must be hidden or obscured. [FIPS Publication 200, Minimum Security Requirements for Federal Information Systems}	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.		Assurance that information is not disclosed to unauthorized individuals, processes, or devices.		The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 13335-1:2004]
Controllability	A measure of how difficult it is to provide inputs to a system to drive its execution.	Modified Secure Software Assurance Guide	Controllability is a measure of how difficult it is to provide inputs to the system to drive its execution. *How difficult it is to cause a system to be in a given state or sequence of states…*	How difficult it is to cause a system to be in a given state or sequence of states...					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Correctness	(1) The degree to which software is free from faults in its specification, design, and implementation. (2) The degree to which software, documentation, or other items meet specified requirements. (3) The degree to which software, documentation, or other items meet user needs and expectations, whether specified or not.	IEEE 610.12-1990						(1) The degree to which software is free from faults in its specification, design, and implementation. (2) The degree to which software, documentation, or other items meet specified requirements. (3) The degree to which software, documentation, or other items meet user needs and expectations, whether specified or not.	For specified security requirements, the representation of a product or system that shows the implementation of the requirement is correct. ISO/IEC 1st WD 21827: 2006-02-07
Covert Channels	Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an IS security policy.	CNSSI 4009	Covert channels are “abnormal” means of communication using such means as timing of overt messages, locations in messages not normally used (e.g. unused bits in packet headers), or (unavailability of resources to convey messages.	Meaning the "software shall contain no function other than those explicitly specified", or "any unspecified function present in the application must be completely isolated and contained so that it cannot be inadvertently executed".			Unintended and/or unauthorized communications path that can be used to transfer information in a manner that violates an IS security policy. See overt channel and exploitable channel.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Critical Software	Software whose failure could have an impact on security, safety, or could cause large financial or social loss. See high-consequence software.	IEEE Std 1012-1986		Safety-critical software is high-consequence software in which a failure could result in the loss of human life.				Software whose failure could have an impact on safety, or could cause large financial or social loss.	
Denial of Service (DoS)	Prevention of authorized access to a system resource or the delaying of system operations and functions.	ISO/IEC FDIS 18028-1			The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending on the service provided.)		An action or series of actions that (1) prevents access to a software system by its intended/authorized users; (2) causes the delay of its time-critical operations; or (3) prevents any part of the system from functioning		Prevention of authorized access to a system resource or the delaying of system operations and functions. ISO/IEC FDIS 18028-1

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Dependability	Integrating concept that encompasses the following attributes - reliability, safety, maintainability, integrity, availability. When addressing security, additional attributes have great prominence - confidentiality and accountability.	Avizienis, Algirdas, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-Mar. 2004.	A qualitative "umbrella" term. Integrating concept that encompasses the following attributes - reliability (continuity of correct service); safety (absence of catastrophic consequences on the user(s) and the environment); maintainability (ability to undergo modifications and repairs...); integrity (absence of improper system alterations); availability (readiness for service). When addressing security, an additional attribute has great prominence - confidentiality, i.e., the absence of unauthorized disclosure of information.						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Dictionary Attack	Attack on a cryptosystem that employs a search of a given list of passwords NOTE -- A dictionary attack on a password-based system can use a stored list of specific password values or a stored list of words from a natural language dictionary.	ISO/IEC FDIS 11770-4: 2006-01-09		An attacker may either manually or programmatically attempt common passwords to gain entry into a system or multiple systems.					Attack on a cryptosystem that employs a search of a given list of passwords NOTE -- A dictionary attack on a password-based system can use a stored list of specific password values or a stored list of words from a natural language dictionary.
Directory Traversal Attack	An HTTP exploit that may allow attackers access to restricted directories and execute commands outside of the web server's root directory, sometimes called a dot dot attack.	Matt Bishop		Occurs when an attacker tries to access restricted files a web service uses.					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Emergent Properties	A property that can appear when a number of entities operate in an environment, forming more complex behaviors as a collective.	DHS		The concept of an emergent property originates from complexity theory, and is elaborated in the Technical Cooperation Programmed Joint Systems and Analysis Group Technical Panel 4 (JSA-TP4) report entitled Systems Engineering for Defence Modernisation (see Appendix B). However, as Fabio Boschetti et al observe in “Defining and Detecting Emergence in Complex Networks” (see Appendix B), “no standard definition of emergence is currently available in the literature.”					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Error	The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.	IEEE 610.12-1990						The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition.	
Event	An occurrence of some specific data, situation, or activity.	ISO/IEC TR 15947							An occurrence of some specific data, situation, or activity.
Exploratory Testing	Simultaneous learning, test design, and test execution; that is, the tests are not defined in advance in an established test plan, but are dynamically designed, executed, and modified.	Abran 2004	Simultaneous learning, test design, and test execution; that is, the tests are not defined in advance in an established test plan, but are dynamically designed, executed, and modified. [SWEBOK Guide (p. 5-5]						
Fail Safe	Pertaining to a system or component that automatically places itself in a safe operating mode in the event of a failure. See also fault secure and fault tolerance.	IEEE 610.12-1990					Automatic protection of the system or component from compromise when a hardware or software failure is detected.	Pertaining to a system or component that automatically places itself in a safe operating mode in the event of a failure. See also fault secure, fault tolerance	

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Failure	The inability of a system or component to perform its required functions within specified performance requirements.	IEEE 610.12-1990						The inability of a system or component to perform its required functions within specified performance requirements.	
Fault	The adjudged or hypothesized cause of an error.	Avizienis, Algirdas, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing,” IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, Jan.-Mar. 2004.						A defect in a hardware device or component.	

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Fault Tolerance	The ability of a system or component to continue normal operation despite the presence of hardware or software faults.	IEEE 610.12-1990						The ability of a system or component to continue normal operation despite the presence of hardware or software faults.	
Forceful Browsing Attack	Occurs when the attacker attempts to access the web server directly instead of following links to gain access to restricted parts in the Web server directory.			Attempt to detect web services that are not explicitly publicized					
Formal Development	Software development strategy that formally proves the system's design specifications.	CNSSI 4009					Software development strategy that formally proves the system's design specifications.		
Formal Methods	Mathematical argument which verifies that the system satisfied mathematically described properties.	CAS, Sam Redwine	"Refers to mathematically rigorous techniques and tools for the specification, design and verification of software and hardware systems…'[Langley 2005]	Formal methods apply mathematical techniques and precise mechanisms for reasoning to the design, production, and evaluation of software.			Mathematically argument which verifies that the system satisfied a mathematically described security policy.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Formal Proof	The complete and convincing mathematical argument that presents the full logical justification for each proof step and for the truth of the theorem or set of theorems to be proved.	CNSSI 4009					The complete and convincing mathematical argument that presents the full logical justification for each proof step and for the truth of the theorem or set of theorems to be proved.		
Formal Verification	The process of using formal proofs to demonstrate the consistency between the formal requirements specification or formal security policy of a system and its formal design specification (design verification) or between its formal design specification and its high-level implementation (implementation verification).	CNSSI 4009					The process of using formal proofs to demonstrate the consistency between the formal requirements specification or formal security policy of a system and its formal design specification (design verification) or between its formal design specification and its high-level implementation (implementation verification).		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Grayware	A term applied to a wide range of applications on a computer to track or report (or both) information as personal as passwords or as general as how often visitors use an organization's website. Applications that fall into this category include joke applications and key loggers.								
Government Off the Shelf (GOTS)	Software and hardware products that are developed by the technical staff of the government agency for which it is created or by an external entity, but with funding and specification from the agency. Because agencies can directly control all aspects of GOTS products, these are generally preferred for government purposes.	CAS				GOTS software is typically developed by the technical staff of the government agency for which it is created.	GOTS software often requires special features and assurances that are not found in typical COTS software. These additional features and assurances are usually developed with U.S. Government cooperation and results in software that contain domestic and/or international restrictions.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
High-Consequence Software	See critical software.			High-consequence software systems are those in which a failure could result in serious harm to a human being in the form of loss of life, physical injury or damage to health, loss of political freedom, loss of financial well-being, or disastrous damage to the human's environment.					
Ilities	Aspects or non-functional requirements. They are so-named because most of them end in "-ility." A subset of them (Reliability, Availability, Serviceability, Usability, and Installability) are together referred to as RASUI.								

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Information Assurance	Protection and defense of 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.	CNSSI 4009	A catch all term for all that is done to assure security of information. The level of assurance or justifiable confidence one has in that security.		Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Source: CNSSI-4009		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.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Information Assurance Architecture	The functions of developing IA operational, system and technical architecture for the purpose of specifying and implementing new or modified IA capabilities within the IT environment.	CNSSI 4009	An abstract description (used among others by the U.S. Department of Defense (DoD)) of a combination of information assurance (IA) solutions for a system or set of systems that assigns and portrays IA roles, identifies behavior among a set of information technology assets, and prescribes rules for interaction and interconnection to ensure security and taking advantage of supporting IA infrastructures. [DoD Instruction 8500.0, Enclosure 2].				***Activity that aggregates*** the functions of developing IA operational, system and technical architecture for the purpose of specifying and implementing new or modified IA capabilities within the IT environment. [DoD Directive 8100.1, 19. Sept 2002]		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Infrastructure Assurance	Ensuring that the organization has a planned and documented assurance case and security architecture as well as tangible policies, processes, and methodologies that establish operational assurance, analysis, and response management.	CBK	Infrastructure assurance involves processes that apply, coordinate, and sustain Operational Assurance, Analysis, and Response Management. Infrastructure assurance ensures that the organization has a planned and documented assurance case and security architecture as well as tangible policies, processes, and methodologies that establish operational assurance, analysis, and response management.						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Integrity	Property that data has not been altered or destroyed in an unauthorized manner.	ISO/IEC 18028-2: 2006-02-01	Absence of improper system alterations.	SDLC - Software must not be able to be corrupted or intentionally subverted by authorized or unauthorized actors during the Software's development or execution.	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.		Quality of an IS reflecting the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.	The degree to which a system or component prevents unauthorized access to, or modification of, computer programs or data.	The property of safeguarding the accuracy and completeness of assets. [ISO/IEC 13335-1:2004] Property that data has not been altered or destroyed in an unauthorized manner.[ISO/IEC 18028-2: 2006-02-01]
Integrity Attack	Attack whose objective is to exploit the targeted application or services to make unauthorized changes to information accessed/handled by the application/service.	Security in the Lifecycle Guide		Objective of an integrity attack is to exploit the targeted application or services to make unauthorized changes to information accessed/handled by the application/service					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Justifiable Confidence	The actions, arguments and evidence that provides a basis for justified reduction in uncertainty.		Level of confidence.						
Least Privilege	Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of that subject's authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of a component or system.	CNSSI 4009					Principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of that subject's authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of a component or system.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Logic Bomb	Malicious software that will adversely affect systems under certain conditions such as at a certain time or upon receipt of a certain packet.	CBK	Weakens or destroys systems under certain conditions such as at a certain time or upon receipt of a certain packet.	Malicious code that is left dormant until the web service reaches a certain state, at which point the malicious code is executed; Malicious logic inserted into a deployed web service in order to perform an unwanted action when a specific criterion is met. (e.g., at a particular time, or when a rigging action is performed.			Resident computer program triggering an unauthorized act when particular states of an IS are realized.		
Maintainability	The ease with which a software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment.	IEEE 610.12-1990	Ability to undergo modifications and repairs					The ease with which a software system or component can be modified to correct faults, improve performance or other attributes, or adapt to a changed environment.	

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Malicious Software	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, availability or accountability of an information system.	CAS, Sam Redwine			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 affects a host. [SP 800-53 & CNSSI 4009]		*Malicious Code* - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS.		
Malware	See Malicious Software		Malicious software such as viruses.		A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of an information system of the victim's data, applications, or operating systems or of otherwise annoying or disrupting the victim. [SP-800-53]				Malicious software, such as a virus or a trojan horse, designed specifically to damage or disrupt a system.ISO/IEC FDIS 18028-1: 2006-03-31

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Mathematically Rigorous	Describes the specifications used in formal methods as well-formed statements in a mathematical logic and that the formal verifications are rigorous deductions in that logic.	Langley, Formal Methods, 2005.	The specifications used in formal methods are well-formed statements in a mathematical logic that the formal verification s are rigorous deductions in that logic."						
Model Checking	A method to algorithmically verify formal systems, achieved by verifying if the model, often derived from a hardware or software design, satisfies a formal specification.	CAS, Sam Redwine							
Modified Off the Shelf (MOTS)	A MOTS (either modified or modifiable off-the-shelf, depending on the context) whose code has been modified.	NASA				Typically a COTS product whose source code can be modified.			

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Multiple Independent Levels of Security (MILS)	An architecture that offers strong enforcement and control of local (microprocessor centric to include multi-core) and end-to-end data-isolation, information flow, resource sanitization and damage limitation security policies. This is achieved through the use of layered reference monitors which are Non-bypassable, Evaluatable, whose security critical decisions are Always-invoked, and which are Tamper-proof (NEAT).	Van Fleet 2005 NSA	Bottom separation layer providing information flow and data isolation facilities so higher layers can define and enforce policies themselves [Vanfleet 2005]						
Non-Repudiation	The ability to prove an action or event has taken place, so that this event or action cannot be repudiated.	ISO/IEC 13888-1	Actors being unable to effectively deny (repudiate) an action.	Pertains to the ability to prevent users (humans and processes) from disproving or denying responsibility for actions they performed while interacting with the software. (FIPS 200 Minimum Security Requirements for Federal Information Systems.	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Source: CNSSI-4009		Assurance that sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.		The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later [ISO/IEC 13888-1; ISO IS 7498-2]

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Observability	The degree to which you can observe what happened internally and externally to the system.	Redwine, CAS 2006	Observability is a measure of how difficult it is to capture and determine whether the test results are correct.						
OTS (Off the Shelf)	Existing software that is potentially available. Includes COTS, MOTS, and GOTS.	Redwine, CAS 2006	This includes COTS (Commercial off the Shelf Software) and other OTS (Off the Shelf Software). This may also include (for governments) GOTS (Government off the Shelf Software and NDI (Non-developmental Items) [Also see FAR Subpart 2.1 for a US federal government definition of commercial items].			Ready-made software used "as-is" within a system. Includes COTS and MOTS (Modified Off-the-Shelf) and GOTS.			

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Outsourcing	The delegation of operations or jobs from internal production within a business to an external entity.	Redwine, CAS 2006	Outsourcing implies that the work is being done within the acquirer's organization and a subsequent decision is made to contract out the work to an outside organization. [FAR 2005, PART 10: Market Research]						
Penetration Testing	Security testing in which evaluators attempt to violate security properties of a system.	Redwine, CAS 2006	Attack testing that involves having persons try to break the software. Aims to violate specified or expected security usually by imitating techniques used by real-world malicious attackers. [Whitaker 2004][Flickenger 2003]	Where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise that application, its data, or its environmental resources.			Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.		
Pharming	A method of redirecting Internet traffic to a fake web site through domain spoofing.	McAfee							

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Phishing	Tricking individuals into disclosing sensitive personal information through the use of e-mails that appear to originate from a trusted source.	NIST	A method of tricking people into giving up their personal information. Deceptive emails requesting entry of information on fake web pages.		Tricking individuals into disclosing sensitive personal information through deceptive computer-based means. Source: SP 800-83				
Plausible Deniability			Plausible deniability is when there is a shred of doubt as to whether an attack was on purpose and conducted by who seems to be behind it.	When malicious developers who purposely plant defects in software can always claim that the defects were simple errors.					
Predictability	The degree that a correct prediction of a system's outcome can be made.	Redwine, CAS 2006	A measure of how difficult it is to determine what a test's outcome should be.	Means that the functionality, properties, attributes, and behaviors of the software will always be demonstrated in that software when it executes under anticipated operating conditions.					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Predictable Execution	Execution with a high level of predictability.	Redwine, CAS 2006		The software, when executed, performs its functions in the manner in which they are intended to be performed, and does not perform any unintended functions.					
Pre-existing Software									
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Definition 2- Freedom from observation, intrusion or attention of others.	ISO/IEC 18028-2: 2006-02-01 Definition 2- Redwine, CAS 2006.							Right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. ISO/IEC 18028-2: 2006-02-01
Protection Profile	An implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs.	ISO/IEC 15408-1					Common Criteria specification that represents an implementation-independent set of security requirements for a category of Target of Evaluations that meets specific consumer needs.		An implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs (adapted from ISO/IEC 15408-1)

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Reference Monitor	The security engineering term for IT functionality that - 1) controls all access, 2) cannot be by-passed, 3) is tamper-proof, and 4) provides confidence that the other three items are true.	Redwine, CAS 2006	A tamperproof, trusted access or interface point that mediates access to objects within a system. [Bishop 2003]	Enables stronger isolation of processes and data stored at different mandatory access levels, and strongly constrains accesses and interactions among those entities.	The security engineering term for IT functionality that - 1) controls all access, 2) cannot be by-passed, 3) is tamper-resistant, and 4) provides confidence that the other three items are true. Source: SP 800-33		Concept of an abstract machine that enforces Target of Evaluation (TOE) access control policies.		
Reliability	The ability of a system or component to perform its required functions under stated conditions for a specified period of time.	IEEE 610.12-1990	Continuity of correct service. Depends on the distributions of inputs and or the patterns of use.	The ability of a system or component to perform its required functions under stated conditions for a specified period of time; “the capability of a computer, or information or telecommunications system, to perform consistently and precisely according to its specifications and design requirements, and to do so with high confidence. [IEEE 610.12-1990]		Software reliability is often defined as the extent to which a program can be expected to perform intended functions with required precision over a given period of time. The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions. [NASA-GB-8719.13]		The ability of a system or component to perform its required functions under stated conditions for a specified period of time.	The property of consistent intended behavior and results. ISO/IEC 13335-1: 2004-11-15

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Residual Risk	The risk remaining after risk treatment.	ISO/IEC 13335-1			The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat. [SP 800-33]		Portion of risk remaining after security measures have been applied.		The risk remaining after risk treatment.ISO/IEC 13335-1: 2004-11-15
Risk	The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence [ISO/IEC 13335-1:2005]. Combination of the probability of an event and its consequence. [ISO/IEC Guide 73:2002]	ISO/IEC 13335-1:2005			The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.	Combined effect of the likelihood of an unfavorable occurrence and the potential impact of that occurrence	Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.		The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence [ISO/IEC 13335-1:2005].

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Risk Management	A process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. Includes all of the activities that an organization carries out in order to manage and control risk.	ISO/IEC 27001	Risk management is the process of planning, assessing risk, mitigating risks, monitoring risk mitigation activities, and adjusting the risk mitigation activities, as appropriate, based on the results of the monitoring activity. [NIST SP 800-30]	The process of identifying, controlling, and eliminating or minimizing (i.e., "mitigating") the uncertain events that may affect the security of the software.	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information systems. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies or regulations. [SP 800-53]	Process of assessing potential risks and reducing those risks within budget, schedule, and other constraints.	Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment.		A process that includes four activities: risk assessment, risk acceptance, risk treatment, and risk communication. Includes all of the activities that an organization carries out in order to manage and control risk.

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Robustness	The degree to which a component or system can function correctly in the presence of invalid inputs or stressful environmental conditions, including inputs or conditions that are intentionally and maliciously created.	IEEE Std 610.12-1990						The degree to which a component or system can function correctly in the presence of invalid inputs or stressful environmental conditions, including inputs or conditions that are intentionally and maliciously created [IEEE Std 610.12-1990]	
Rootkit	A set of tools designed to conceal an attacker and offer a backdoor after the attacker has compromised the machine. [Hoglund 2004].								

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Safety	Absence of catastrophic consequences on the user(s) and the environment.	DHS	Absence of catastrophic consequences on the user(s) and the environment.			concerned with the possibility of catastrophic failure of systems in such a way as to compromise the safety of people or property, or result in mission failure. Software safety is definable only in the system context. Software has no inherent dangers; however, systems controlled or monitored by software do fail, and some failures of some systems will have safety impacts. To the extent that system failures can be caused or fail to be prevented by software, there is a need for an activity called			

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Script Kiddie	A hacker who only uses software created by others without knowing what they are or how they work, for the purpose of compromising computer accounts and files, and for launching attacks on whole computer systems.		Novice hackers; technically unsophicated.						
Scumware	Malicious or undesirable software.								
Secure Software	Software that realizing- with justifiably high confidence but not guaranteeing absolutely – a substantial set of explicit security properties and functionality including all those required for its intended usage.	Redwine, Samuel T., Jr., and Noopur Davis (Editors). Processes for Producing Secure Software: Towards Secure Software. vols. I and II. Washington, D.C.: National Cyber Security Partnership, 2004.	"Highly secure software realizing – with justifiably high confidence but not guaranteeing absolutely – a substantial set of explicit security properties and functionality including all those required for its intended usage." [Redwine 2004. p.2]	For software to be secure it must avoid defects in its implementation that introduce vulnerabilities regardless of whether the majority of development involves either from-scratch coding or integration/assembly of acquired or reused software components.					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Secure Software Project Management	Systematic, disciplined, and quantified" application of management activity that ensures the software being developed conforms to security policies and meets security requirements.	Abran 2004	The "systematic, disciplined, and quantified" application of management activity to include the "planning, coordinating, measuring, monitoring, controlling, and reporting" that ensures the software being developed conforms to security policies and meets security requirements [Abran 2004]						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Security	All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability and authenticity.	Redwine, CAS 2006	A composite of confidentiality, integrity, and availability. Requires the simultaneous existence of 1) availability for authorized actions only, 2) confidentiality, and 3) integrity with "improper" meaning unauthorized. Axizienis 2204, p.13. All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability. [ISO/IEC 13335-1].	True software security is only achievable only when all known aspects of the software are understood, and verified to be predictably correct.					All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. [ISO/IEC 13335-1]

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Security Accreditation	The security related official management decision given to authorize operation of a system.	Redwine, CAS 2006	The official management decision given to authorize operation of an information system and to explicitly accept the risk to an organization's (and by implication interconnecting organizations') operations (including mission, functions, image, or reputation), assets, or individuals based on the implementation of an agreed-upon set of security controls. [DoD Instruction 8500.2, Enclosure 2].		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. Source: 800-37.				
Security Architecture	Computer security model referring to the underlying computer architectures, protection mechanisms, distributed computing environment security issues, and formal models that provide the framework for information systems security policy.								

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. Source: SP 800-37.	NIST	Means the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.		The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. Source: SP 800-37.				

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Security Certification	“Security certification” may apply to a software system as in the case of the Common Criteria or FIPS-140 or may mean 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 [NIST Special Publication 800-37].	NIST 800-37	“Security certification” may apply to a software system as in the case of the Common Criteria or FIPS-140 or may mean 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 [NIST Special Publication 800-37].						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Security Goals	The five security goals are confidentiality, availability, integrity, accountability, and assurance. [SP 800-27A]	NIST			The five security goals are confidentiality, availability, integrity, accountability, and assurance. [SP 800-27A]				
Security Relevant									
Service Level Agreement (SLA)	Contract that defines the technical support or business performance objectives including measures for performance and consequences for failure the provider of a service can provide its clients. ISO/IEC FDIS 18043: 2006-03-14.	ISO/IEC FDIS 18043: 2006-03-14.	Service Level Agreements (SLAs) are suggestive of a method for expressing and contractually agreeing to specific measures of performance [Gaines & Michael 2005]						Contract that defines the technical support or business performance objectives including measures for performance and consequences for failure the provider of a service can provide its clients. ISO/IEC FDIS 18043: 2006-03-14.

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Sniffer	A sniffer is a software tool for auditing and identifying network traffic packets.	CNSSI 4009		Act of monitoring network traffic exchanged between web services to capture sensitive plaintext data such as unencrypted passwords and security configuration information transmitted in SOAP, UDDI (Universal Description, Discovery, and Integration), WSDL, and other such messages.	Sniffer software observes and records network traffic. Source: SP 800-61.		A sniffer is a software tool for auditing and identifying network traffic packets.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Software Acquisition	To obtain software development services or software products whether by contract or by other means (e.g., downloading open source software from the internet, etc.)		"acquisition" means the acquiring of software development services or software products whether by contract or by other means, e.g., downloading open source software from the Internet. For the U.S. Federal government, also see the FAR Subpart 2.101(b)(2) definition of acquisition. In addition, for purposes of this document, "acquisition" applies to functions across the entire acquisition framework and the software development life cycle, including development, integration, testing, operations, maintenance and disposition, as well						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Software Architecture	A design that assigns and portrays roles and behavior among all IT assets.	Modified Secure Software Assurance Guide (DHS)_	Software architecture is a design plan that assigns and portrays roles and behavior among all IT assets. Software security-related roles and behaviors must be integrated into the overall software architecture in a manner that facilitates the software assurance case.	Should include countermeasures to compensate for vulnerabilities or inadequate assurance in individual components or intercomponent interfaces.					
Software Assurance	ModifyCNSSI 4009- The level of confidence that software is free of vulnerabilities, either intentionally or unintentionally designed or inserted during software development and/or the entire software lifecycle.	CNSSI 4009	Refers to the assurance of any property or functionality of software.			The planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures.	Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.		
Software Intensive System									

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Software Protection Initiation									
Software Pedigree	Background/lineage of the software being acquired.	Secure Software Assurance Guide(DHS).	Background/lineage of the software being acquired.						
Software Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [NIST SP 800-53]	CNSSI 4009	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a software information system to protect the confidentiality, integrity, and availability of the system and its information.		The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.		The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [NIST SP 800-53]		
Spamming	Sending of bulk unsolicited messages which on receipt cause adverse effects on the availability of information system resources.	ISO/IEC FDIS 18028-1: 2006-03-31	Unsolicited bulk e-mail. Recipient who clicks on links to spam messages may put themselves at risk for spyware, viruses, and other malware.						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Spyware	Programs that observe and report on users; any technology that aids in gathering information about a person or organization without their knowledge.		Any technology that aids in gathering information about a person or organization without their knowledge. Spyware is placed on a computer to secretly gather information about the user and relay it to advertisers or other interested parties.	Monitors selected system activities and reports them to a remote entity.					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Standards	An agreement among any number of organizations that defines certain characteristics, specification, or parameters related to a particular aspect of computer technology.	IEEE Std 100-1996, The IEEE Standard Dictionary of Electrical and Electronic Terms, Sixth Edition.	Standards are usually more specific statements of behavior intended to implement a policy or policies. An agreement among any number of organizations that defines certain characteristics, specification, or parameters related to a particular aspect of computer technology. [IEEE Std 100-1996, The IEEE Standard Dictionary of Electrical and Electronic Terms, 6th edition]						

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Subversion	Changing (process or) product so as to provide a means to compromise security;	Anderson, E. A., C. E. Irvine, and R. R. Schell. “Subversion as a threat in information warfare.” Journal of Information Warfare, 3:51 - - 64, 2004.	Changing (process or) product so as to provide a means to compromise security; used to describe subversion of people (e.g. developers), subversion of machines or network nodes, subversion of software, and of other things.	When software is vulnerable to compromise.					
Sustainment			Substainment involves processes that continue to assure that software satisfies its intended purpose after initial deployment and during operations.						
Systematic Risk	Chance of loss that is predictable under relatively stable circumstances. (fire, wind, or flood produce losses, that in the aggregate, over time can be accurately predicted despite short-term fluctuations.	Risk and Insurance Management Society Magazine							
System Level Profile (synonym)									

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Target of Evaluation	An IT product or system and its associated guidance documentation that is the subject of an evaluation.	ISO/IEC 15408-1: 2005-10-01							An IT product or system and its associated guidance documentation that is the subject of an evaluation.ISO/IEC 15408-1: 2005-10-01
Technical Specification									
Testing	Propose to CNSSI 4009- Testing is an activity performed for evaluating product quality, and for improving it, by identifying defects and problems. The verification of behavior of a program on a finite set of test cases, suitably selected from the usually infinite executions domain, against the expected behavior. Five types of testing. Penetration, Interoperability, Acceptance, Vulnerability, and Functionality.	Abran 2004	Testing is an activity performed for evaluating product quality, and for improving it, by identifying defects and problems. Software testing consists of the dynamic verification of the behavior of a program on a finite set of test cases, suitably selected from the usually infinite executions domain, against the expected behavior. [Abran 2004]	To verify that the software does not manifest any unexpected behaviors in execution.		Process of exercising or evaluating software by manual or automated means to demonstrate that it satisfies specified requirements or to identify differences between expected and actual results.			

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Threat	A potential cause of an incident that may result in harm to a system or organization.	ISO/IEC 13335-1: 2004-11-15			Any circumstance or event with the potential to adversely impact agency 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.		Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.		A potential cause of an incident that may result in harm to a system or organization.

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Threat Model	Threat modeling is the analysis, assessment and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.	CNSSI 4009	A number of techniques, issues, and benefits result from carefully analyzing proposed designs and identifying and reducing vulnerabilities. [Swiderski and Snyder 2004] gives substantial coverage to vulnerability analysis through the term threat modeling, which gives coverage to vulnerability analysis which covers both threat analysis and vulnerability analysis.	A detailed textual description and graphical depiction of significant threats to the software system/application being modeled. [Frank Swiderski and Window Snyder of Microsoft]			Threat modeling is the analysis, assessment and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.		
Threat Source					Either: 1) intent and method targeted at the intentional exploitation of a vulnerability; or 2)a situation and method that may accidentally trigger a vulnerability.				

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Trapdoor	Hidden software or hardware mechanism used to circumvent security controls. Synonymous with backdoor.								
Trojan Horse	Malicious program that masquerades as a benign application.	ISO/IEC FDIS 18043: 2006-03-14	Provides remote access to a system through a back door or open port.	Malicious program that appears to do something non-malicious while launching a separate background process to perform malicious functions under the privileges of a valid service.	Trojan horses are self-replicating programs that seem to have a useful purpose, but in reality has a different, malicious purpose. Source: NIST 800-61.		Trojan horses are programs that contain hidden code allowing the unauthorized collection, falsification, or destruction of information. Also see malicious code.		Malicious program that masquerades as a benign application.
Trust	A relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not violate the given security policy.	ISO/IEC 13888-1: 2004-06-01	Accepting the risk that an entity which can harm you, will not do so. Bishop 2003						A relationship between two elements, a set of activities and a security policy in which element x trusts element y if and only if x has confidence that y will behave in a well defined way (with respect to the activities) that does not violate the given security policy.ISO/IEC 13888-1: 2004-06-01

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Trustworthiness	"An entity is trustworthy if there is sufficient credible evidence leading one to believe that it will meet a set of give requirements."	Bishop 2003	"An entity is trustworthy if there is sufficient credible evidence leading one to believe that the system will meet a set of give requirements." [Bishop 2003]	The software can be trusted to contain no exploitable vulnerabilities or subversive logic, either maliciously or unintentionally inserted.	The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. Source: SP 800-79.				
Unsystematic Risk	Chance of loss that is predictable in the aggregate because it results from difficult forces to predict. (recession, unemployment, war-related events, etc.)	Risk and Insurance Management Society Magazine							
Virus	Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.	CNSSI 4009	A program or programming code that replicated by being copied or initiating its copying. A virus attaches itself to and becomes part of another executable program: delivery mechanism for malicious code or for denial of service attack.	Malicious program that attaches itself to web service programs, modifies them, then propagates when the infected program is executed.	A self-replicating program that runs and spreads by modifying other programs or files. Source: 800-61.		Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Vulnerability	A weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats. [ISO/IEC 13335-1: 2004-11-15]	ISO/IEC 13335-1: 2004-11-15	A weakness in software exploitable by an attacker.	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited; a characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat"—when that definition is applied to software. [CNSS 4009, White House CIAO]	Weakness in an information system, system security procedures, internal controls, or implementation that cold be exploited or triggered by a threat source. Source: SP 800-53.		Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited.		A *vulnerability* is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harme d by one or more threats. ISO/IEC 13335-1: 2004-11-15
WSDL Scan	See Directory Traversal Attack			A knowledgeable attacker may be able to locate web services that have been removed from the pre-generated WSDL and subsequently access them.					

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Watermarking	[Process to] embed information into software in a manner that makes it hard to remove by an adversary without damaging the software's functionality.	Atallah, Mikhail, Bryant, Eric, and Styz, Martin, "A Survey of Anti-Tamper Technologies," Crosstalk – The Journal of Defense Software Engineering, Nov 2004.	[Process to] embed information into software in a manner that makes it hard to remove by an adversary without damaging the software's functionality. [Atallah, Bryant and Sytz 2005]						
Weakness									

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.	SANS	A self-replicating computer program, similar to a computer virus. Unlike a virus, a worm is self-contained and does not need to be part of another program to propagate itself. Worms frequently exploit the file transmission capabilities found on many computers: self-propagating delivery mechanism for malicious code or for a Denial of Service attack that effectively shuts down service to users.	Malicious that propagates itself over a network without the help of a human user, and which is self-contained.	A self-replicating, self-propagating, self contained program that uses networking mechanisms to spread itself. Source: SP 800-61.		See Malicious Code- Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS.		

Term	Preferred Definition	Reference	Secure Software Assurance Guide (DHS)	Security in the Software Lifecycle Guide (DHS)	NIST Glossary of Key Information Security Terms	NASA Software Assurance STD 2201-93 /Goddard Glossary	CNSSI 4009 National IA Glossary	IEEE Sw Engineering Terms STD 610.12-1990	International Standards Organization (ISO)
Wrappers			Common method of incorporating “new” technology or behavior into legacy code or software libraries by intercepting calls to the legacy code and enhancing the characteristics of the legacy software within the wrapper code. [Birman 1996]	A popular means of encapsulating and isolating high-risk acquired or reused software so as to prevent if from negatively affecting the security of the application in which it is used.					