

Recommendation for Space Data System Practices

INFORMATION SECURITY GLOSSARY OF TERMS

RECOMMENDED PRACTICE

CCSDS 350.8-M-3

MAGENTA BOOK

February 2024

Recommendation for Space Data System Practices

**INFORMATION SECURITY
GLOSSARY OF TERMS**

RECOMMENDED PRACTICE

CCSDS 350.8-M-3

MAGENTA BOOK

February 2024

AUTHORITY

Issue:	Recommended Practice, Issue 3
Date:	February 2024
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the email address below.

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). Current versions of CCSDS documents are maintained at the CCSDS Web site:

<http://www.ccsds.org/>

Questions relating to the contents or status of this document should be sent to the CCSDS Secretariat at the email address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d’Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People’s Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Science Policy Office (BELSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- Egyptian Space Agency (EgSA)/Egypt.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Netherlands Space Office (NSO)/The Netherlands.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.8-G-1	Information Security Glossary of Terms, Informational Report, Issue 1	November 2012	Original issue, superseded
CCSDS 350.8-M-2	Information Security Glossary of Terms, Recommended Practice, Issue 2	February 2020	Issue 2, superseded
CCSDS 350.8-M-3	Information Security Glossary of Terms, Recommended Practice, Issue 3	February 2024	Current issue

CONTENTS

<u>Section</u>	<u>Page</u>
1 INTRODUCTION	1-1
1.1 PURPOSE	1-1
1.2 SCOPE	1-1
1.3 APPLICABILITY	1-1
1.4 RATIONALE	1-1
1.5 REFERENCES	1-1
2 OVERVIEW	2-1
3 GLOSSARY OF INFORMATION SECURITY TERMS	3-1

1 INTRODUCTION

1.1 PURPOSE

This document is issued to provide a central source of information security terms and their respective definitions. It is intended that this document will be included as a normative reference in all CCSDS security documents and any CCSDS documents referencing information security.

1.2 SCOPE

This document provides a glossary of information security terms which can be used by all CCSDS document authors.

1.3 APPLICABILITY

This document is applicable to all document authors requiring definitions for information security terms. It may be included as a normative reference in any document requiring the definitions of information security terms.

1.4 RATIONALE

In the past, each CCSDS security-related document generated and included its own glossary of information security terms. Often, because different sources of definitions were consulted, the definitions between documents were not consistent. The document-specific generation of such glossaries also consumed valuable resources. In order to minimize resource utilization and to ensure definition consistency, this document has been created for use as a normative reference by CCSDS document authors.

1.5 REFERENCES

The following publications contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All publications are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the publications indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS publications.

- [1] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. International Standard, ISO 7498-2:1989. Geneva: ISO, 1989.

- [2] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. 3rd ed. International Standard, ISO/IEC 27001:2022. Geneva: ISO, 2022.
- [3] *Information Technology—Security Techniques—Code of Practice for Information Security Controls*. 3rd ed. International Standard, ISO/IEC 27002:2022. Geneva: ISO, 2022.
- [4] *Committee on National Security Systems (CNSS) Glossary*. Revised. CNSSI No. 4009. Fort Meade, Maryland: CNSS, March 2, 2022.
- [5] *Glossary of Key Information Security Terms*. Edited by Richard Kissel. Rev. 2. NIST IR 7298. Gaithersburg, Maryland: NIST, May 2013 [withdrawn].
- [6] Elaine Barker. *Recommendation for Key Management—Part 1: General*. Revision 4. National Institute of Standards and Technology Special Publication 800-57. Gaithersburg, Maryland: NIST, January 2016.
- [7] *Security and Privacy Controls for Federal Information Systems and Organizations*. Rev. 4 (Updated 1/22/2015). National Institute of Standards and Technology Special Publication 800-53 Rev. 4. Gaithersburg, Maryland: NIST, April 2013.
- [8] *DOD Dictionary of Military and Associated Terms*. Washington, DC: U.S. Department of Defense, April 2018.
- [9] *Glossary of INFOSEC and INFOSEC Related Terms*. Compiled by Corey D. Schou. Pocatello, Idaho: Idaho State U Simplot Decision Support Center, 1996.
- [10] *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*. 5th ed. International Standard, ISO/IEC 27000:2018. Geneva: ISO, 2018.
- [11] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303. Reston, Virginia: ISOC, December 2005.
- [12] *Information Technology—Security Techniques—Encryption Algorithms—Part 4: Stream Ciphers*. 2nd ed. International Standard, ISO/IEC 18033-4:2011. Geneva: ISO, 2011.
- [13] *Software Assurance Standard*. w/Change 1. NASA-STD-8739.8. Washington, DC: NASA, July 28, 2004.
- [14] *Security Requirements for Cryptographic Modules*. Change Notice 2, 12/3/2002. Federal Information Processing Standards Publication 140-2. Gaithersburg, Maryland: NIST, May 25, 2001.
- [15] William Stallings. *Cryptography and Network Security: Principles and Practice*. 8th ed. London: Pearson Education, 2020.

- [16] Elaine Barker, Allen Roginsky, and Richard Davis. *Recommendation for Cryptographic Key Generation. Revision 2*. National Institute of Standards and Technology Special Publication 800-133. Gaithersburg, Maryland: NIST, June 2020.
- [17] Scott Rose, et al. *Zero Trust Architecture. Revision 2*. National Institute of Standards and Technology Special Publication 800-207. Gaithersburg, Maryland: NIST, August 2020.
- [18] Ramaswamy Chandramouli. *Implementation of DevSecOps for a Microservices-based Application with Service Mesh*. National Institute of Standards and Technology Special Publication 800-204C. Gaithersburg, Maryland: NIST, March 2022.
- [19] Tom Karygiannis, et al. *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. National Institute of Standards and Technology Special Publication 800-98. Gaithersburg, Maryland: NIST, April 2007.
- [20] Anoop Singhal, Theodore Winograd, and Karen Scarfone. *Guide to Secure Web Services*. National Institute of Standards and Technology Special Publication 800-95. Gaithersburg, Maryland: NIST, August 2007.
- [21] *Secure Software Development Life Cycle for Space Systems*. Draft Informational Report. Consultative Committee for Space Data Systems, Washington D.C.: CCSDS, forthcoming.
- [22] Shashi Banzal. *Data and Computer Network Communication*. Bangalore: Firewall Media/Laxmi Publications Pvt. Ltd., 2007.
- [23] Terry Ritter. "Ritter's Crypto Glossary and Dictionary of Technical Cryptography." 2007 August 16. Cyphers by Ritter. <http://ciphersbyritter.com/GLOSSARY.HTM>.
- [24] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." May 4, 2022. The White House. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>.
- [25] Jon Boyens, et al. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. Rev 1. National Institute of Standards and Technology Special Publication 800-161. Gaithersburg, Maryland: NIST, May 2022.
- [26] *Information Security, Cybersecurity, and Privacy Protection: Guidance on Managing Information Security Risks*. 4th ed. ISO/IEC 27005:2022. Geneva: ISO, 2022.
- [27] *Space Engineering—Spacecraft On-Board Control Procedures*. ECSS-E-ST-70-01C. Noordwijk, The Netherlands: ECSS Secretariat, 16 April 2010.

- [28] “STRIDE model.” 8/25/2022. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model>. (1/23/2024)
- [29] Elaine Barker, Dennis Branstad, and Miles Smid. *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*. National Institute of Standards and Technology Special Publication 800-152. Gaithersburg, Maryland: NIST, October 2015.
- [30] *Secure Hash Standard (SHS)*. Federal Information Processing Standards Publication 180-4. Gaithersburg, Maryland: NIST, August 2015.

2 OVERVIEW

This document is intended to provide a set of information security terms and their definitions for use as a normative reference in CCSDS documents. The intent is to have a single source of information security terms and definitions. This is desirable so that definitions are not duplicated and do not vary across CCSDS documents.

All of the definitions included in this document were acquired from authoritative sources such as ISO/IEC, NIST, and others which are listed in the normative references. Where available and appropriate for the CCSDS community, ISO/IEC definitions are given the highest priority for inclusion. All of the individual definitions are referenced back to their source.

This glossary ensures the consistency of the definitions across CCSDS.

3 GLOSSARY OF INFORMATION SECURITY TERMS

air gap: An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control). Reference [4].)

access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (Reference [1].)

access control list, ACL: A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. (Reference [5].)

access control mechanism: Those mechanisms which are used to enforce a policy of limiting access to a resource to only those users who are authorized. (Reference [1].)

accountability: (1) The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (2) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. (Reference [5].)

accreditation: Formal declaration by a senior official that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. (Reference [4].)

accreditation authority: Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. (Reference [5].)

active threat: The threat of a deliberate unauthorized change to the state of the system. (Reference [1].)

advanced encryption standard, AES: A symmetric block cipher using cryptographic key sizes of 128, 192, and 256 bits used to encrypt and decrypt data in blocks of 128 bits. (Reference [4].)

advanced key processor, AKP: A cryptographic device that performs all cryptographic functions for a management client node and contains the interfaces to 1) exchange information with a client platform, 2) interact with fill devices, and 3) connect a client platform securely to the primary services node. (Reference [5].)

advanced persistent threats, APT: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). (Reference [5].)

NOTE – These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (Reference [5].)

adversary: Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (Reference [5].)

anti-jam: The measures taken to ensure that transmitted information can be received despite deliberate jamming attempts. (Reference [4].)

anti-spoof: Countermeasures taken to prevent the unauthorized use of legitimate Identification & Authentication (I&A) data, however it was obtained, to mimic a subject different from the attacker. (Reference [5].)

anti-tamper: Systems engineering activities intended to prevent physical manipulation or delay exploitation of critical program information in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering. (Reference: [4].)

asymmetric key algorithm: (See *public key cryptographic algorithm*.)

asset: A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information employed, owned, or operated by domestic, foreign, public, or private sector organizations. (Reference [4].) Anything that has value to the organization. (Reference [3].)

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. (Reference [5].)

assured software: Computer application that has been designed, developed, analyzed, and tested using processes, tools, and techniques that establish a level of confidence in it. (Reference [5].)

attack: Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. (Reference [10].)

audit: An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational

procedures, and to recommend necessary changes in controls, policies, or procedures. (Reference [1].)

audit trail: Data collected and potentially used to facilitate a security audit. (Reference [1].)

authenticate: To verify the identity of a user, user device, or other entity. (Reference [5].)

authentication: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. (Reference [4].) (See also *peer-entity authentication* and *data origin authentication*.)

authentication code: A cryptographic checksum based on an Approved security function (also known as a Message Authentication Code [MAC]). (Reference [5].)

authentication mechanism: Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system. (Reference [5].)

authenticity: Property that an entity is what it claims to be. (Reference [10].)

authority: Person(s) or established bodies with rights and responsibilities to exert control in an administrative sphere. (Reference [5].)

authorization: The granting of rights, which includes the granting of access based on access rights. (Reference [1].)

availability: The property of being accessible and useable upon demand by an authorized entity. (Reference [4].)

block cipher: A symmetric key cryptographic algorithm that transforms a block of information at a time using a cryptographic key. (Reference [5].)

NOTE – For a block cipher algorithm, the length of the input block is the same as the length of the output block. (Reference [5].)

block cipher algorithm: A family of functions and their inverses that is parameterized by a cryptographic key; the function maps bit strings of a fixed length to bit strings of the same length. (Reference [5].)

bulk encryption: The simultaneous (protocol-transparent) encryption of all channels of a multichannel telecommunications link. (Reference [4].)

certificate: A digitally signed document that binds a public key with an identity. The certificate contains, at a minimum, the identity of the issuing certification authority (CA), the user identification information, and the user's public key. (Reference [4].)

certification: The comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the

extent to which a particular design and implementation meets a set of specified security requirements. (Reference [4].)

certificate authority, CA: Trusted entity authorized to create, sign, and issue public key certificates. By digitally signing each certificate issued, the user's identity is certified, and the association of the certified identity with a public key is validated. (Reference [4].)

certification authority: (See *certificate authority*.)

certificate management: Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed. (Reference [5].)

certificate policy, CP: A specialized form of administrative policy tuned to electronic transactions performed during certificate management. (Reference [5].)

NOTE – 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. (Reference [5].)

certificate revocation list, CRL: A list of revoked public key certificates created and digitally signed by a Certification Authority. (Reference [5].)

challenge-response-protocol: An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a secret (often by hashing the challenge and a shared secret together, or by applying a private key operation to the challenge) to generate a response that is sent to the verifier. (Reference [5].)

NOTE – The verifier can independently verify the response generated by the Claimant (such as by re-computing the hash of the challenge and the shared secret and comparing to the response, or performing a public key operation on the response) and establish that the Claimant possesses and controls the secret. (Reference [5].)

cipher: Series of transformations that converts plaintext to ciphertext using the Cipher Key. (Reference [5].)

cipher suite: Negotiated algorithm identifiers. Cipher suites are identified in human-readable form using a mnemonic code. (Reference [5].)

cipher text: Data produced through the use of encipherment. The semantic content of the resulting data is not available. (Reference [1].)

classification: A ‘scheme’ for information within an organization, with processes intended to ‘indicate value of assets’ in ‘consistent’ terms, based on ‘legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification’, in a way that ensures ‘information receives an appropriate level of protection’, and that supports ‘information labelling’. (Reference [3].)

cloud computing: A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Reference [5].)

NOTE – Cloud computing allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). (Reference [5].)

common criteria, CC: Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Reference [4].)

common control: A security control that is inherited by one or more organizational information systems. (Reference [5].)

common vulnerabilities and exposures (CVE): A list of entries, each containing an identification number, a description, and at least one public reference, for publicly known computer system vulnerabilities. (Reference: [4].)

common weaknesses enumeration (CWE): A community-developed formal list or dictionary of common software weaknesses that can occur in software's architecture, design, code or implementation that can lead to exploitable security vulnerabilities. (Reference [4].)

computer cryptography: Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information. (Reference [5].)

computer forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (Reference [5].)

computer network attack, CNA: Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Reference [5].)

computer network defense, CND: Actions taken to defend against unauthorized activity within computer networks. (Reference [5].)

NOTE – CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities. (Reference [5].)

configuration management: (See *configuration control*.)

configuration control: Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation. (Reference [4].)

confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (Reference [1].)

contingency key: Key held for use under specific operational conditions or in support of specific contingency plans. (Reference [4].)

countermeasures: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. (Reference [4].)

covert channel: An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. (Reference [5].)

covert channel analysis: Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information. (Reference [5].)

credential: An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber. (Reference [5].)

cryptanalysis: Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. (Reference [6].)

cryptology: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. (Reference [1].)

cryptographic algorithm: A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output. (Reference [6].)

cryptographic boundary: An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all hardware, software, and/or firmware components of a cryptographic module. (Reference [6].)

cryptographic key: A binary string used as a secret parameter by a cryptographic algorithm. (Reference [5].)

cryptographic module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. (Reference [5].)

crypto period: The time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. (Reference [6].)

cyber attack: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (Reference [5].)

cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. (Reference [5].)

cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks. (Reference [5].)

cyberspace: The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information systems, industrial control systems, networks, and embedded processors and controllers. (Reference [4].)

data integrity: The property that data has not been changed, destroyed, or lost in an unauthorized manner. (Reference [4].)

data origin authentication: The corroboration that the source of data received is as claimed. (Reference [1].)

decipherment: The reversal of a corresponding reversible encipherment. (Reference [1].)

decryption: (See *decipherment*.)

defense-in-depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. (Reference [4].)

denial of service, DOS: The prevention of authorized access to resources or the delaying of time-critical operations. (Reference [1].)

DevSecOps: (Development, Security, and Operations) A culture and set of practices with automation tools to drive increased collaboration, trust, shared responsibility, transparency, autonomy, agility, and automation across the key stakeholders responsible for delivering software, including development, operations, and security organizations. (Reference [18].)

digital certificate: (See *certificate*.)

digital signature: Data appended to, or a cryptographic transformation (see *cryptography*) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient. (Reference [1].)

digital signature algorithm: Asymmetric algorithms used for digitally signing data. (Reference [5].)

discretionary access control, DAC: An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability. (Reference [4].)

eavesdropper: A party that secretly receives communications intended for others. (Reference [19].)

electronic credentials: Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. (Reference [5].)

embedded cryptographic system: Cryptosystem performing or controlling a function as an integral element of a larger system or subsystem. (Reference [5].)

embedded cryptography: Cryptography engineered into an equipment or system whose basic function is not cryptographic. (Reference [5].)

encipherment: (See *encryption*.)

encryption: The cryptographic transformation of data (see *cryptography*) to produce ciphertext. (Reference [1].)

encryption algorithm: A set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. (Reference [4].)

end-to-end encipherment: Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. (Reference [1].)

end-to-end security: The safeguarding of information in an information system from its point of origin to its intended destination. (Reference [4].)

ephemeral key: A cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message or session). (Reference [6].)

exploitation: Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. (Reference [8], definition 2.)

firewall: A system designed to prevent unauthorized access to or from a private network. (Reference [4].) Firewalls can be implemented in both hardware and software, or a combination of both.

flooding: An attack that attempts to cause a failure in a system by providing more input than the system can process properly. (Reference [5].)

forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. (Reference [4].)

formal method: Software engineering method used to specify, develop, and verify the software through application of a rigorous mathematically based notation and language. (Reference [4].)

formal security policy: Mathematically-precise statement of a security policy. (Reference [5].)

frequency hopping: The repeated switching of frequencies during radio transmission according to a specified algorithm to minimize unauthorized interception or jamming of telecommunications. (Reference [4].)

fuzz testing: [Input of invalid data into an application or process.] Similar to fault injection in that invalid data is input into the application via the environment, or input by one process into another process. Fuzz testing is implemented by tools called fuzzers, which are programs or script that submit some combination of inputs to the test target to reveal how it responds. (Reference [20].)

gateway: Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures. (Reference [5].)

hacker: Unauthorized user who attempts to or gains access to an information system. (Reference [4].)

hash function: A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties: 1) (One-way) it is computationally infeasible to find any input which maps to any pre-specified output; and 2)

(Collision-resistant) it is computationally infeasible to find any two distinct inputs that map to the same output. (Reference [6].)

hash-based message authentication code, HMAC: A message authentication code that uses a cryptographic key in conjunction with a hash function. (Reference [4].)

identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. (Reference [4].)

identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable. (Reference [4].)

identity-based access control: Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity. (Reference [5].)

identity-based security policy: A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. (Reference [1].)

incident response: The remediation or mitigation of violations of security policies and recommended practices. (Reference [4].)

information assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Reference [4].)

information disclosure: Access to information by an unauthorized entity. (Reference [21].)

information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Reference [5].)

information security architecture: An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. (Reference [5].)

information security policy: Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information. (Reference [5].)

information system: A set of applications, services, information technology assets, or other information-handling components. (Reference [10].)

information systems security engineer: Individual assigned responsibility for conducting information system security engineering activities. (Reference [4].)

information systems security engineering: Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration. (Reference [4].)

initialization vector, IV: A vector used in defining the starting point of a cryptographic process. (Reference [6].)

insider threat: The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities. (Reference [7].)

integrity: (See *data integrity*.)

interconnection security agreement, ISA: Written management authorization to interconnect information systems based upon acceptance of risk and implementation of established controls. (Reference [4].)

Internet Protocol Security, IPsec: Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. (Reference [5].)

NOTE – IPsec also includes protocols for cryptographic key establishment. (Reference [5].)

intranet: A computer network, especially one based on Internet technology, that an organization uses for its own internal (and usually private) purposes and that is closed to outsiders. (Reference [4].)

intrusion detection system, IDS: Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations). (Reference [4].)

intrusion prevention system: System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (Reference [5].)

jamming: An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable. (Reference [5].)

key: (See *cryptographic key*.)

key confirmation: A procedure to provide assurance to one party that another party actually possesses the same keying material and/or shared secret. (Reference [6].)

key derivation: A function in the lifecycle of keying material; the process by which one or more keys are derived from a shared secret and other information. (Reference [6].)

key distribution: The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key. (Reference [6].)

Key-Encryption-Key, KEK: Key that encrypts or decrypts other keys for transmission or storage. (Reference [4].)

key establishment: A function in the lifecycle of keying material; the process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). (Reference [6].)

key exchange: The process of exchanging public keys (and other information) in order to establish secure communications. (Reference [4].)

key length: The length of a key in bits; used interchangeably with 'Key size'. (Reference [6].)

key management: The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. (Reference [6].)

key management policy: The key management policy is a high-level statement of organizational key management policies that identifies high-level structure, responsibilities, governing standards and recommendations, organizational dependencies and other relationships, and security policies. (Reference [6].)

key pair: Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and 2) even knowing one key, it is computationally infeasible to discover the other key. (Reference [5].)

key recovery: A function in the lifecycle of keying material; mechanisms and processes that allow authorized entities to retrieve or reconstruct keying material from key backup or archive. (Reference [6].)

key revocation: A function in the lifecycle of keying material; a process whereby a notice is made available to affected entities that keying material should be removed from operational use prior to the end of the established cryptoperiod of that keying material. (Reference [6].)

key stream: (*See stream cipher.*)

key strength: A measure of resistance to attack often expressed in bits. If the strength is S bits, then it is expected that (roughly) 2^S basic operations are required to break the algorithm or system. (Reference [16].)

key transport: A key establishment procedure whereby one party (the sender) selects and encrypts the keying material and then distributes the material to another party (the receiver). (Reference [6].)

key update: A function performed on a cryptographic key in order to compute a new, but related, key. (Reference [4].)

key validity: (*See crypto period.*)

key wrapping: A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key. (Reference [6].)

keying material: The data (e.g., keys and IVs) necessary to establish and maintain cryptographic keying relationships. (Reference [6].)

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. (Reference [5].)

link-by-link encipherment, link encryption: The individual application of encipherment to data on each link of a communications system. (Reference [1].)

malicious code, 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. (Reference [7].)

man-in-the-middle-attack, MitM: A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. (Reference [5].)

masquerading: The pretense by an entity to be a different entity. (Reference [4].)

master key: A symmetric master key is used to derive other symmetric keys (e.g., data encryption keys, key wrapping keys, or authentication keys) using symmetric cryptographic methods. (Reference [6].)

meaconing: A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. (Reference [8].)

memorandum of understanding/agreement, MOU/A: A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. With respect to security, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. (Reference [4].)

message authentication code, MAC: A cryptographic checksum that results from passing data through a message authentication algorithm. (Reference [4].)

message digest: A cryptographic checksum typically generated for a file that can be used to detect changes to the file. Synonymous with hash value/result. (Reference [4].)

multiple encryption: (Also known as *superencryption*) Repeated use of an encryption function with different keys to produce a more complex mapping from plaintext to ciphertext. (Reference [15].)

multi-factor authentication: (Also known as ‘strong authentication’.) Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). (Reference [7].)

mutual authentication: The process of both entities involved in a transaction verifying each other. (Reference [5].)

mutual suspicion: Condition in which two information systems need to rely upon each other to perform a service, yet neither trusts the other to properly protect shared data. (Reference [5].)

nonce: (Also known as ‘number used once’.) A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks. (Reference [4].)

non-repudiation: (See also *repudiation*.) 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. (Reference [4].)

one-time password: A password used only once and then permanently discarded.

over-the-air key distribution, OTAD: Providing electronic key via over-the-air rekeying, over-the-air key transfer, or cooperative key generation. (Reference [5].)

over-the-air key transfer, OTAT: Electronically distributing key without changing traffic encryption key used on the secured communications path over which the transfer is accomplished. (Reference [5].)

over-the-air rekeying, OTAR: Changing traffic encryption key or transmission security key in remote cryptographic equipment by sending new key directly to the remote cryptographic equipment over the communications path it secures. (Reference [5].)

padding: (1) (bit padding) The addition of one or more extra bits to a transmission or storage unit to make it conform to a standard size. (Reference [22].) (2) In classical cryptography, random data added to the start and end of messages so as to conceal the length of the message, and the position where coding actually starts. In more conventional computing, some additional data needed to fill-out a fixed-size data structure. This meaning also exists in cryptography, where the last block of a fixed-size block cipher often must be padded to fill the block. (Reference [23].)

passive threat: The threat of unauthorized disclosure of information without changing the state of the system. (Reference [1].)

password: A string of characters (letters, numbers and other symbols) that are used to authenticate an identity, to verify access authorization or to derive cryptographic keys. (Reference [6].)

peer-entity authentication: The corroboration that a peer entity in an association is the one claimed. (Reference [1].)

penetration testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. (Reference [7].)

phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. (Reference [5].)

plaintext: Unencrypted information. (Reference [4].)

policy decision point, PDP: A system entity that makes authorization decisions for itself or for other system entities that request such decisions. (Reference [4].)

policy enforcement point, PEP: A system entity that requests and subsequently enforces authorization decisions. (Reference [4].)

post-quantum cryptography: Cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a CRQC or classical computer. (Reference [24].)

private key: In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. (Reference [4].)

private network: (See *intranet*.)

privilege: A right granted to an individual, a program, or a process. (Reference [5].)

privilege management: The definition and management of policies and processes that define the ways in which the user is provided access rights to enterprise systems. It governs the management of the data that constitutes the user's privileges and other attributes, including the storage, organization, and access to information in directories. (Reference [5].)

pseudorandom number generator, PRNG: An algorithm that produces a sequence of bits that are uniquely determined from an initial value called a seed. The output of the PRNG 'appears' to be random, i.e., the output is statistically indistinguishable from random values. A cryptographic PRNG has the additional property that the output is unpredictable, given that the seed is not known. (Reference [5].)

public key: A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign. (Reference [4].)

public key cryptographic algorithm: A cryptographic algorithm that uses two related keys: a public key and a private key. (Reference [6].)

NOTE – The two keys have the property that determining the private key from the public key is computationally infeasible. (Reference [6].)

public key infrastructure, PKI: Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. (Reference [4].)

random number generator, RNG: A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected. (Reference [4].)

recovery key: (*See contingency key.*)

rekey: To change the value of a cryptographic key that is being used in a cryptographic system/application. (Reference [5].)

replay attacks: An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. (Reference [4].)

repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication. (Reference [1].)

residual risk: The risk remaining after risk treatment. (Reference [10].)

resource: A device, data element, or file for which access is requested. Also known as protected resource and as an object. (Reference [4].)

risk: Effect of uncertainty on objectives. (Reference [10].) Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. (Reference [4].)

risk analysis: Systematic use of information to identify sources and to estimate the risk. (Reference [2].)

risk appetite: The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value. (Reference [25].)

risk assessment: Overall process of risk identification, risk analysis and risk evaluation (Reference [10].)

risk management: 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 system. (Reference [5].)

NOTE – Risk management 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. (Reference [5].)

risk mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. (Reference [5].)

risk owner: Person or entity with the accountability and authority to manage a risk. (Reference [26].)

risk treatment: Process of selection and implementation of measures to modify risk. (Reference [5].)

rule-based security policy: A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. (Reference [1].)

safe mode: (*See survival mode.*)

secret (symmetric) key infrastructure, SKI: Cryptographic key infrastructure used to generate and distribute secret (symmetric) keying material such as master keys, key encryption keys, and traffic protection keys.

secret key algorithm: (*See symmetric encryption algorithm.*)

secret key: A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term ‘secret’ in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. (Reference [4].)

secure channel: A path for transferring data between two entities or components that ensure confidentiality, integrity, and replay protection as well as mutual authentication between the entities or components. The secure channel may be provided using cryptographic, physical, or procedural methods or a combination thereof. (Reference [16].)

secure hash algorithm, SHA: A hash algorithm with the property that is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. (Reference [4].)

secure hash standard: Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. (Reference [30].)

security association, SA: A relationship established between two or more entities to enable them to protect data they exchange. (Reference [5].)

security audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend an indicated changes in control, policy, and procedures. (Reference [1].)

security controls: 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. (Reference [4].)

security hardening: The process of eliminating a means of attack by patching vulnerabilities and turning off nonessential services. (Reference [29].)

security mechanism: A device designed to provide one or more security services usually rated in terms of strength of service and assurance of the design. (Reference [5].)

security operations center (SOC): 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. (Reference [7].)

security parameters index, SPI: An arbitrary 32-bit value that is used by a receiver to identify the security association to which an incoming packet is bound. (Reference [11].)

security perimeter: A physical or logical boundary that is defined for a system, domain, or enclave, within which a particular security policy or security architecture is applied. (Reference [5].)

security plan: Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. (Reference [5].)

security policy: The set of criteria for the provision of security services (see also *identity-based security policy* and *rule-based security policy*). (Reference [1].) A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. (Reference [5].)

security protocol: An abstract or concrete protocol that performs security-related functions. (Reference [4].)

security requirements: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. (Reference [5].)

security test and evaluation, ST&E: Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system. (Reference [4].)

sensitivity: A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. (Reference [4].)

session key: (See *ephemeral key*.)

shared secret: A secret value that has been computed using a key agreement scheme and is used as input to a key derivation function. (Reference [6].)

signed data: Data on which a digital signature is generated. (Reference [5].)

software assurance: The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures. (Reference [13].)

spoofing: (See *masquerading*.)

spread spectrum: A telecommunications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum. (Reference [4].)

static key: A key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establishment scheme. Contrast with an ephemeral key. (Reference [6].)

stream cipher: An encryption mechanism that uses a keystream to encrypt a plaintext in bitwise or block-wise manner. (Reference [12].)

STRIDE: (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) A model of threats, used to help reason and find threats to a system. It is used in conjunction with a model of the target system that can be constructed in parallel. This includes a full breakdown of processes, data stores, data flows, and trust boundaries. (Reference [28].)

superencryption: (See *multiple encryption*.)

survival mode: Configuration of a spacecraft in which it can remain safely without ground segment intervention for a specified period. (Reference [27].)

NOTE – Survival mode is also commonly known as safe mode. In survival mode, typically all non-essential on-board units or subsystems are powered off, either to conserve power or to avoid interference with other subsystems, and the spacecraft can be (automatically) oriented to a particular attitude with respect to the sun.

symmetric encryption algorithm: Encryption algorithms using the same secret key for encryption and decryption. (Reference [5].)

symmetric key: (See *secret key*.)

system: Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (Reference [4].)

system integrity: The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. (Reference [5].)

tampering: An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data. (Reference [4].)

threat: A potential violation of security. (Reference [1].) Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (Reference [5].)

threat analysis: The examination of information to identify the elements comprising a threat. (Reference [4].)

threat assessment: Formal description and evaluation of threat to a system. (Reference [4].)

threat intelligence: Information feed or feeds about general threats and active malware operating on the internet. This could also include specific information about communication seen from the device that may be suspect (such as queries for possible malware command and control nodes). (Reference [17].)

threat modeling: A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment. (Reference [7].)

threat source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. (Reference [5].)

traffic analysis: Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence. (Reference [4].)

traffic encryption key, TEK: Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text. (Reference [4].)

traffic protection key: (*See traffic encryption key.*)

transport layer security, TLS: An authentication and security protocol widely implemented in browsers and Web servers. (Reference [5].)

trap door: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. (Reference [4].)

Trojan horse: A program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. (Reference [4].)

trust: Confidence that an entity, to which trust is applied, will perform in a way that will not prejudice the security of the system of which that entity is a part. (Reference [9].)

trust anchor: A public key and the name of a certification authority that is used to validate the first certificate in a sequence of certificates. (Reference [6].)

NOTE – The trust anchor's public key is used to verify the signature on a certificate issued by a trust anchor certification authority. The security of the validation process depends upon the authenticity and integrity of the trust anchor. Trust anchors are often distributed as self-signed certificates. (Reference [6].)

unauthorized disclosure: (*see information disclosure*)

validation: Confirmation, through the provision of objective evidence, that the requirements (2.63) for a specific intended use or application have been fulfilled. (Reference [10].)

verification: Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. (Reference [10].)

virtual private network, VPN: Protected information system link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line. (Reference [4].)

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. (Reference [4].)

vulnerability: Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy and result in a security breach. (Reference [4].)

vulnerability analysis: (See *vulnerability assessment*.)

vulnerability assessment: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (Reference [4].)

worm: A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. (Reference [4].)

X.509 certificate: The X.509 public-key certificate or the X.509 attribute certificate, as defined by the ISO/ITU-T X.509 standard. (Reference [6].)

X.509 public key certificate: A digital certificate containing a public key for entity and a name for the entity, together with some other information that is rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. (Reference [6].)

zero-day attack: An attack that exploits a previously unknown hardware, firmware, or software vulnerability. (Reference: [4].)

zero fill: To fill unused storage locations in an information system with the representation of the character denoting '0'. (Reference [5].)

zero trust, ZT: 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. (Reference [17].)

zero trust architecture, ZTA: An enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. (Reference [17].)

zeroization: A method of erasing electronically stored data, cryptographic keys, and Critical Security Parameters (CSPs) by altering or deleting the contents of the data storage to prevent recovery of the data. (Reference [14].)