The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

INFORMATION SECURITY GLOSSARY OF TERMS

DRAFT RECOMMENDED PRACTICE

CCSDS 350.8-P-2.1

PINK SHEETS

February 2023

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Standards

INFORMATION SECURITY GLOSSARY OF TERMS

DRAFT RECOMMENDED PRACTICE

CCSDS 350.8-P-2.1

PINK SHEETS
February 2023

[2] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. 2nd ed. International Standard, ISO/IEC 27001:2013. Geneva: ISO, 2013.

[3] *Information Technology—Security Techniques—Code of Practice for Information Security Controls*. 2nd ed. International Standard, ISO/IEC 27002:2013. Geneva: ISO, 2013.

[4a] *Committee on National Security Systems (CNSS) Glossary*. Revised. CNSSI No. 4009. Fort Meade, Maryland: CNSS, April 6, 2015.

[4b] *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 Gaithersburg, Maryland: NIST, May 2013 [withdrawn].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.

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 [4a].)

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].)

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 [4b].) 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].)

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: ~~A standard (ISO/IEC 15408) providing~~Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Reference [4a].)

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

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 [4a].)

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 [4b].)

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

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].)

cryptography: 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 [4b].)

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

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 [4a].)

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

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)

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 [4a].)

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 [4a].)

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

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 [4a].)

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 private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). (Reference [2].)

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 with the organizations). (Reference [4a].)

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 stream: Sequence of symbols (or their electrical or mechanical equivalents) produced in a machine or auto-manual cryptosystem to combine with plain text to produce cipher text, control transmission security processes, or produce key. (Reference [4a].)

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 [4a].)

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 software, malware: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an ~~IS~~information system. (Reference [4a].)

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 [4a].)

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 [4a].)

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

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 [4a].)

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 [4a].)

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 [4a].)

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: ~~Fill data required by certain cipher modes~~Appending extra bits to a data string. (Reference [12].)

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].)

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 [4a].)

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

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

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 [4a].)

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 [4a].)

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 [4a].)

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 [4a].)

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 [4a].)

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 [2].)

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

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 [4a].)

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

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 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].)

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 [4a].)

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 [4a].)

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 [4a].)

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].)

superencryption: (See *multiple encryption.*)

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

symmetric key: (See *secret key*.)

system: (See *information system.*)

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].)

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 [4a].)

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

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].)

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

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

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].)

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].)

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].)