CISSP Glossary

1. **Abstraction** - The process of removing characteristics from something to reduce it to a set of essential characteristics for the purpose of creating specific groups, classes, or roles for the assignment of security controls, restrictions, or permissions as a collective. SOURCE: Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2018.
2. **Acceptance Testing** - Testing used to verify a system satisfies the stated criteria for functionality and a required security capabilities of a product. It is used to ensure a customer is satisfied with the functionality of the software. SOURCES: Abernathy & McMillan, 2018; Chapple, Stewart, & Gibson, 2018.
3. **Access Aggregation** - Associated with privilege creep, this technique also functions as a reconnaissance tool by attackers to collect multiple pieces of non-sensitive data, which is combined to gain greater access across more systems. SOURCES: Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2018.
4. **Access Control -** A method to control an authorized subject's communication with or access to objects, resources, and physical facilities. This security-based control determines how hardware, software, and organizational policies and procedures are used to identify subjects to provide authentication, verification, and authorization while monitoring and recording the subject's access attempts. SOURCES: CNSSI-4009; Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2018.
5. **Access Control List (ACL)** - A list associated with a specific object, specifying what operations can be done by a subject; and a system resource access control determining either implicit or explicit allow or deny to a resource. SOURCE: CNSSI-4009.
6. **Access Control Lists (ACLs)** - Columns in a control matrix, listing the permissions granted to a subject (user, group, process) to access an object or resource, and the type of access allowed to the subject. SOURCE: NISTIR 7298, r2.
7. **Access Control Matrix** - A table in which each row represents a subject, each column represents an object, and each entry is a set of "access rights" a specific subject can take on a specific object. Columns are the ACL. Capabilities are the rows. SOURCE: NISTIR 7316.
8. **Access Control Policy** - High-level security policy requirements specifying how access is managed and which subjects may access objects, information, and resources, and under what circumstances. SOURCE: NIST SP 800-192.

9. **Access Point (AP)** - A wireless transmitter and receiver that logically connects wireless client devices operating in the infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network. SOURCE: NIST SP 800-121, r2.
10. **Account Management** - Process of requesting, establishing, issuing, and closing user accounts. Includes tracking users and their access authorizations and managing these functions. SOURCE: NIST SP 800-12, r1.
11. **Accounting** - A process that ensures the actions of an entity may be traced uniquely to that entity (subject/user) to be held accountable for their actions or inactions. SOURCES: NIST SP 800-57, Pt. 1., r4; Abernathy & McMillian, 2018.
12. **Accountability** - The security goal generating the requirement for actions of an entity to be traced uniquely to that entity to support non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. SOURCES: NIST SP 800-27 and NIST SP 800-160.
13. **Accreditation** - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. SOURCES: FIPS 200; NIST SP 800-37.
14. **Acoustical Systems** - Detection system that uses strategically placed microphones to detect any sound made during a forced entry. SOURCE: Harris & Maymi, 2018.
15. **Acrylic Glass** - Glass made of polycarbonate acrylic, which is stronger than regular glass but produces toxic fumes when burned. SOURCE: Harris & Maymi, 2018.
16. **Active Vulnerability Scanner (AVS)** - An active scanner that blocks dangerous IP addresses and attacks. SOURCE: Abernathy & McMillan, 2018.
17. **ActiveX** - Microsoft's component object model (COM) technology used in web applications, which is implemented with Visual Basic, C, C++, and Java. SOURCE: Chapple, Stewart, & Gibson, 2018.
18. **Ad Hoc Mode/Ad Hoc Network** - A wireless network with dynamic connections between devices without the use of an access point or wireless base-station. SOURCE: NIST SP 800-121, r2.
19. **Address Resolution Protocol (ARP)** - A protocol used to obtain a node's physical address, that then resolves the IP address place in a packet to a physical or data link layer 2 MAC/Ethernet address, to which the client can transmit data. SOURCE: NIST SP 800-45, v2, p. A-1.

20. **Administrative Control** - Known also as “soft controls,” a method used by management to control the development process of standards, policies, procedures, and guidelines. Used to screen personnel, conduct security awareness training, monitor system activity, and manage the change control process. SOURCE: Harris & Maymi, 2018.
21. **Administrative Law** - Laws set by the government and published in the Code of Federal Regulations (CFR), which specify the performance and conduct standards for banking, communications, environmental controls, healthcare and utilities. SOURCE: Abernathy & McMillian, 2018; Stewart, Chapple, & Gibson, 2018.
22. **Advanced Persistent Threat (APT)** - An adversary with sophisticated expertise and resources allowing it to attack via multiple attack vectors (e.g. cyber, physical, and deception). Attackers repeatedly pursue objectives over extended time periods, adapt to resist detection, and maintain levels of interaction to execute objectives, which include: establish footholds, exfiltration of data, and undermining organizational mission. SOURCE: NIST SP 800-39, p. B-1.
23. **Adware** - Software that tracks internet usage in an attempt to tailor ads and junk emails to a user’s interest. SOURCE: Abernathy & McMillan, 2018.
24. **Advance Encryption Standard (AES)** - A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. This algorithm is a symmetric block cipher that can encipher and decipher in 128-bit blocks using 128-, 192-, 256-bit keys. SOURCES: FIPS 197, p.5; NIST-SP 800-57 Pt.1, r4, p. 23.
25. **Aggregation** - The consolidation of information from different lower security levels to produce potentially useful information at a higher sensitivity level. May also consolidate similar log entries into a single entry containing the number of occurrences of an event. SOURCE: NIST-SP 800-92, p. A-1.
26. **Agile Software Development** - Software development models emphasizing continuous customer feedback and cross-functional teamwork, with the goal of quickly producing new functionality with each product version update or release. SOURCES: Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2015.
27. **Algorithm** - Known also as a cipher, it is a clearly specified mathematical process for computation to produce a specific result to encipher and decipher data. SOURCE: NIST SP 800-107, r1.
28. **Annualized Loss Expectancy (ALE)** - The expected risk factor of an annual threat event. Equation: ALE = SLE x ARO. SOURCE: Abernathy & McMillian, 2018.
29. **Annualized Rate of Occurrence (ARO)** - An estimate of how often a given threat might occur annually. SOURCE: Abernathy & McMillian, 2018.

30. **Application Firewall -** A firewall that uses stateful protocol analysis to analyze network traffic for one or more applications. SOURCE: NIST SP 800-179, p. 118.
31. **Application Layer (Layer 7) -** The layer of the TCP/IP OSI protocol stack that sends and receives data for particular applications such as DNS, HTTP, and SMTP. SOURCE: NIST SP 800-113.
32. **Application Level Gateway (ALG) -** Application specific translation agents that allow an application (like VoIP) on a host in one address realm to connect to its counterpart running on a host in different realm transparently. It may interact with NAT to set up state, use NAT state information, modify application specific payload and perform whatever else is necessary to get the application running across disparate address realms. SOURCE: NIST SP 800-58, p. 59.
33. **Application-Level Gateway Firewall -** A second-generation firewall that filters traffic based on the internet service (the application) used to transmit or received the data. SOURCE: Chapple, Stewart, & Gibson, 2018.
34. **Application Level Proxy -** A type of firewall that performs deep pack inspection and based on Layer 7 communication processes for each application. SOURCE: Abernathy & McMillian, 2018.
35. **Application Programming Interface (API) -** A system access point or library function that has a well-defined syntax and is accessible form application programs or user code to provide well-defined functionality. SOURCE: CSRC Glossary.
36. **Architecture -** The organization of a system, including its components and their interrelationships, along with the principles that guided the system's design and evolution. It is used to convey information about system/solution elements, interconnections, relationships, and behavior at different levels of abstractions and with different scopes. Related to security architecture. SOURCE: NIST SP 800-160, p.101.
37. **Assembly Languages -** Higher-level alternatives to machine language code, which uses mnemonics to represent the basic instruction set of a CPU but still require hardware-specific knowledge. SOURCE: Chapple, Stewart, & Gibson, 2018.
38. **Asset -** Resources of value that an organization possesses or employs. May be any product, process, system, or digital or physical entity that has value to the organization and must be protected. SOURCES: NISTIR 8011 Vol.1, p. B-1; Abernathy & McMillian, 2018.
39. **Asset Valuation -** The process of assigning a monetary value to an asset based on its importance to the organization. Methods to determine value include costs of development, maintenance, administration, support, repair, and replacement. Other valuations may

include public confidence and ownership benefits. SOURCES: Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2018.

40. **Assurance** - Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. NIST SP 800-53, r4., p. B-1.

41. **Asymmetric DSL (ADSL)** - DSL that provides 128 Kbps to 384 Kbps uploads with downloads up to 768 Kbps. SOURCE: Abernathy & McMillian, 2018

42. **Asymmetric Encryption** - An algorithm that uses either complex algorithms or key pairs (one private, one public) to encrypt and decrypt data. SOURCES: NISTIR 7298; CSRC; and Chapple, Stewart, & Gibson, 2018.

43. **Asymmetric Keys** - Two related keys, comprised of a public key and a private key, which are used to perform complementary operations such as encryption and description or signature verification and generation. SOURCE: NIST SP 800-63-3, p. 40.

44. **Asymmetric Mode** - When a specific processor, each time, does work for a specific application or process. SOURCE: Abernathy & McMillian, 2018

45. **Asynchronous Encryption** - Encryption or decryption requests that are processed from a queue. SOURCE: Abernathy & McMillian, 2018.

46. **Asynchronous Transfer Mode (ATM)** - A cell-switching technology that transfers fixed 53 byte cells and uses an established path for the entire communication. It provides guaranteed throughput and is excellent for WAN voice and video-conferencing. SOURCES: Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2018.

47. **Asynchronous Transmission** - Transmission with start and stop bits communicate when each byte is starting and stopping. SOURCE: Abernathy & McMillian, 2018.

48. **Atomicity** - One of four database requirements that mandates that all database transactions must be complete or a transaction fails, meaning the entire transactions must be rolled back. SOURCES: Abernathy & McMillian, 2018; Chapple, Stewart, & Gibson, 2018.

49. **Attack** - An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality. SOURCE: NIST SP 800-82 r2, p. B-1.

50. **Attacker** - A party, including an insider, who acts with malicious intent to compromise a system. SOURCE: NIST SP 800-63-3, p. 40.

51. **Attack Vector** - A segment of the communication path that an attack uses to access a vulnerability. SOURCE: Abernathy & McMillian, 2018.

52. **Attenuation** - The gradual reduction of the amplitude of a signal, electrical current, or other oscillation as it loses strength due to the distance traveled down a cable. SOURCE: Merriam-Webster.
53. **Attribute** - A quality or characteristic ascribed to someone or something. SOURCE: NIST SP 800-63-3, p. 40.
54. **Attribute-Based Access Control (ABAC)** - Access control based on attributes with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which a subject's access may take place. Many SDN applications use this type of control model. SOURCE: CSRC, 2019.
55. **Auditing** - Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. This includes the use of audit logs and monitoring tools to track all activity. SOURCE: CSRC, 2019.
56. **Auditors** - A member of the organization, usually assigned by the Chief Operations Officer (COO), or an independent entity, who inspects reports and risk assessments from one or more analyzers to ensure than an application or business process meets the security requirements of the organization. SOURCE: CSRC, 2019.

57. **Authentication** - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources. SOURCES: NIST SP 800-63-3, p. 41.; FIPS 200, p.6.
58. **Authentication Factor** - Consisting of three types: Type One - Something you know; Type Two - Something you have; and Type Three - Something you are. SOURCE: NIST SP 800-63-3, p. 41.
59. **Authentication Header (AH)** - A protocol that provides integrity, authentication, and nonrepudiation through IPsec. It provides encryption through encapsulation security protocol (ESP). SOURCES: Abernathy & McMillian, 2018; Stewart, Chapple, & Gibson, 2015.
60. **Authenticator** - The means used to confirm the identity of a user, processor, or device (e.g., user password or token). Example, a subject may attempt to connect to an AP, switch, or remote access server in a RADIUS environment. SOURCES: NIST SP 800-53, r4, p. B-2; Abernathy & McMillian, 2018.
61. **Authorize** - A decision to grant access, typically automated by evaluating a subject's attributes. SOURCE: NIST SP 800-63-3, p. 42.

62. **Authorization** - The right or a permission that it granted to a system entity to access a system resource; the granting of denying of access rights to a subject, program, or process. SOURCE: NIST SP 800-82, r2., p.B-2.
63. **Automatic Private IP Addressing (APIPA)** - A feature of Windows that assigns an IP address to a system should DHCP address assignment fail. The IP address range used by APIPA is 169.254.0.0 - 169.254.255.255. SOURCE: Stewart, Chapple, & Gibson, 2015.
64. **Auxiliary Station Alarm /Auxiliary Alarm System** - An added alarm that can be either locally or centrally placed in a facility, which automatically transmits alarms to local emergency services (fire, police,) and the organization's appropriate headquarters. SOURCES: Abernathy & McMillian, 2018; Stewart, Chapple, & Gibson, 2015.
65. **Availability** - Tenet of the CIA Triad that ensures timely, reliable access to data and information services for authorized users. As a security goal, it generates the requirement for protection against intentional or accidental attempts to perform unauthorized deletion of data or otherwise cause denial of service or data. SOURCES: NIST SP 800-53, r4., p. B-2; NIST SP 800-152; NIST SP 800-33.

66. **Avalanche Effect** - The condition where any changes in the key or plaintext, no matter how minor, will significantly change the ciphertext. SOURCE: Abernathy & McMillian, 2018.
67. **Back door or Backdoor** - Both an undocumented way of gaining access to a computer system and or a malicious program that listens for commands on certain TCP and UDP ports; both pose significant security risks. SOURCE: NIST SP 800-82, r2, p. 77.

68. **BACnet2** - A master/slave industrial control system (ICS) protocol that uses port 47808. SOURCE: Abernathy & McMillian, 2018.
69. **Base Relation** - A table that physically resides/exists and is stored in an SQL database. SOURCE: Freeman, 2014.
70. **Baseband** - A communication medium that supports only a single communication signal at a time and multiple transmission types are assigned time slots to use the same single circuit. SOURCE: Stewart, Chapple, & Gibson, 2015.
71. **Basel II** - In 1974 the ten-country Basel Committee on Banking Supervisions based in Switzerland, established "three pillars" of recommendations to protect banking institutions against financial risk. The pillars define requirements for minimum capital requirements, supervisory review, and market disciple. SOURCE: Bakiciol, et al, (n.d.).

72. **Baseline** - A formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle, used as a security governance reference for performance measures. SOURCE: IEEE 828, 2012.
73. **Baselining** - Monitoring critical resources to determine typical utilization patterns so that significant deviations can be detected. SOURCE: NIST SP 800-61 p. F-1.
74. **Basic Rate ISND (BRI)** - A telecommunications solution that provides three channels, where two channels are each 64 Kbps, each with a 16 Kbps D channel, totaling 144 Kbps. SOURCE: Abernathy & McMillian, 2018.
75. **Bastion Host** - A special purpose computer on a network directly exposed to the internet and where the computer is specifically designed and configured to withstand attacks. SOURCE: CNSSI 4009-2015, p. 11.
76. **Bell-LaPadula model** - A model which uses a formal state transition to describe access controls and how they should perform. As a system transitions between states, the system's security must not be lowered or compromised; uses the simple (read) no read up property and * (star) no write down property, which are used to control the information flow. SOURCE: Harris, & Maymi, 2018.
77. **Best Evidence Rule** - A rule which states documentary evidence (written or recorded) must only be presented in its original form unless a legitimate reason exists for not using the original, which can only be permitted by a judge (the court). SOURCE: Stewart, Chapple, & Gibson, 2015.
78. **Biba Model** - A formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. SOURCE: Harris, & Maymi, 2018.
79. **Biometric Acceptability** - Measurement of the likelihood that users will accept and follow the system. SOURCE: Abernathy & McMillian, 2018.
80. **Biometric Accuracy** - How correct the overall biometric readings will be. SOURCE: Abernathy & McMillian, 2018.

81. **Biometrics** - Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity of, an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. SOURCE: NIST SP 800-32, p. 8.
82. **Biometric Throughput** - The rate at which the biometric system will be able to scan characteristics and complete the analysis to permit or deny access. SOURCE: Abernathy & McMillian, 2018.

83. **Birthday Attack** - A type of brute-force attack where the attacker compares one-way hashes of a password based on a birthday paradox that at least two people out of 253 in a room will statistically have the same birthday. SOURCE: Miessler, 2014.
84. **Black Box Testing** - A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. This method of software testing examines the functionality of an application without peering into its internal structures or workings. This method can be applied to virtually every level of software testing: unit, integration, system, and acceptance. SOURCE: NIST SP 800-192, p. 55.
85. **Blacklisting** - The process used to identify un-authorized software programs from executing on an information system, and the blocking of unacceptable URLs or email senders that have previously been identified as malicious attackers or spammers. A user's ID may also be blocked from accessing system resources. SOURCE: NIST SP 800-53, r4, p3.
86. **Blackout** - A complete and extended loss of electrical power.
87. **Blind Test** - When a testing team conducts an attack on a network, system, or software using only publically available information. The internal security team is alerted to the coming attack. SOURCE: Doraiswamy, 2011.
88. **Block Cipher** - A symmetric-key cryptographic algorithm that transforms one block of information at a time using a cryptographic key; the length of the input block is the same as the length of the output block. SOURCE: NIST SP 800-90A r1, p. 3.
89. **Blowfish** - Created in t 2991, it is a license-free block cipher of 64-bit block with a variable key length of 32 bits to 448 bits, which is faster than DES and IDEA. SOURCE: Schneier, 2019.
90. **Bluejacking** - Hijacking a Bluetooth connection to eavesdrop or extract information from devices. SOURCE: Stewart, Chapple, & Gibson, 2018.
91. **Bluesnarfing** - When an attacker connects to an unsuspecting person's Bluetooth device, to steal personal information such as contacts. SOURCE: Chapple, Stewart & Gibson, 2015.
92. **Bluetooth 802.15** - A wireless protocol that allows two Bluetooth enabled devices to communicate with each other within a short distance, e.g. up to thirty feet. SOURCE: CSRC, 2019.
93. **Border Gateway Protocol (BGP)** - An Internet Engineering Task Force (IETF) path vector standard routing protocol used across the global internet used to establish services such as multicast and VPNs. SOURCE: Cisco, (2019).

94. **Botnet** - A very large collection of computers control by a bot-master across the global internet to attack various target or launch attacks such as DDoS attacks. SOURCE: Norton, 2019.
95. **Breach** - Occurs when an internal or external attacker access information without authorization, then discloses the stolen data (e.g. PII, sensitive information). SOURCE: Symanovich, 2019.

96. **Brewer-Nash (Chinese Wall) Model** - A security model used to prevent conflict of interests by grouping "conflict of interest classes" and restricting permissions by access controls based on the user's previous actions. It was designed to be used in financial institutions. SOURCE: Brewer & Nash, 1989.
97. **Broadcast** - Transmission to all devices in a network without any acknowledgement by the receivers. SOURCE: NIST SP 800-82, r2.
98. **Brownout** - A prolonged drop in electrical power that is below normal voltage. SOURCE: Abernathy & McMillian, 2018.
99. **Buffer Overflow** - A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. CNSSI 4009-2015, p. 13.
100. **Build Security In (BSI)** - An approach of building security into software from the start and making security recommendations with regard to architectures, testing methods, code review, and management processes. SOURCE: Abernathy & McMillian, 2018.
101. **Business Continuity Plan (BCP)** - The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption. SOURCE: NIST SP 800-34 r1., p. G-1.
102. **Business Impact Analysis (BIA)** - Analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. SOURCE: NIST SP 800-34, r1., p.G-1.
103. **Byte** - A string of eight bits. SOURCE: NIST SP 800-106, p. 3.
104. **Cable Lock** - A vinyl-coated steel cable that connects to a laptop and then locks around an object. SOURCE: Abernathy & McMillian, 2018.
105. **Candidate Key** - A subset of attributes, columns, or fields that can be used to uniquely identify any record in a table. SOURCE: Chapple, Stewart & Gibson, 2015.

106. **Capability Maturity Model Integration (CMMI) -** Development model used to determine the maturity of an organization’s processes. SOURCE: Harris & Maymi, 2018.
107. **Capability Table -** A table that specifies access rights a certain subject possesses to access specific objects. Harris & Maymi, 2018.
108. **Capacitance Detector -** A type of proximity detector that emits a measurable magnetic field and sounds an alarm when the field is disrupted; often used in museums. Harris & Maymi, 2018.
109. **Cardinality** - The number of rows in a relational database.
110. **Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) -** A medium sharing method in which each computer signals its intent to transmit data before it actually does, to inform the other systems not to send, to prevent collisions. Harris & Maymi, 2018.

111. **Carrie Sense Multiple Access/Collision Detection (CSMA/CD) -** Medium access method where a system listens for the absence of a carrier tone on the wire to determine if the wire is free, and if so, then transmits data. Harris & Maymi, 2018.
112. **Certificate Authority (CA) -** An entity in a Public Key Infrastructure (PKI) organization that is responsible to authenticate and issue digital certificates to subjects and whose root certificate is included in modern web browsers. SOURCE: NIST SP 800-57, Pt.1, R4, p.6.
113. **Certificate Revocation List (CRL) -** A list of revoked public key certificates created and digitally signed by a CA. SOURCE: CNSSI 4009-2015, p. 15.
114. **Certificate Status Authority (CSA)** - A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate. SOURCE: CNSSI 4009-2015, p. 16.
115. **Certificate Status Server (CSS)** - An authority that provides status information about certificates on behalf of the CA through online transactions (e.g., an online certificate status protocol (OCSP) responder). SOURCE: CNSSI 4009-2015, p. 16.
116. **Certification -** The technical evaluation of a system; the process of evaluating the software for its security effectiveness with regard to the customer’s needs. SOURCE: Abernathy & McMillian, 2018.
117. **Chain of Custody** - A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose of the transfer. SOURCE: CNSSI 4009-2015, p. 17.
118. **Challenge Handshake Authentication Protocol (CHAP)** - A system of challenges and response mechanisms used between a server and a client. A server sends a random challenge, which the client encrypts and returns to the server. The server decrypts the

challenge value to pair it with the original value sent. If the values are the same, the server grants access to the client. Harris & Maymi, 2018.

119. **Channel Service Unit/Data Service Unit (CSU/DSU) -** Required when digital equipment will be used to connect a LAN to a WAN via a T1 or T3 line. It is used to modulate the signals between routers, switches, and multiplexers. Harris & Maymi, 2018.
120. **Chief Executive Officer (CEO) -** Person primarily responsible for due diligence, executive management decisions, and ultimate responsibility for the organization.
121. **Chief Financial Officer (CFO) -** Person responsible for executive management of an organization's budget and finances.
122. **Chief Information Officer (CIO) -** Executive management person responsible for ensuring technology supports the organization's objective. SOURCE: NIST SP 800-53, r4., p. B-3.
123. **Chosen Ciphertext Attack -** An attack in which the attacker has the ability to decrypt chosen portions of the ciphertext message. SOURCE: Chapple, Stewart, & Gibson, 2018.
124. **Cipher Block Chaining (CBC) -** An operation that used DES to XOR unencrypted output of one block with the input of the next block, n+1. SOURCE: Pound, 2019.
125. **Cipher Feedback (CFB) -** A mode in which the DES algorithm is used to encrypt the preceding block of cipher; the block is XORed with the next block of plaintext to produce the next block of ciphertext. SOURCE: Chapple, Stewart, & Gibson, 2018.
126. **Ciphertext -** An encrypted message. SOURCE: Pound, 2019.
127. **Class A Fire Extinguisher -** Used on ordinary combustibles.
128. **Class B Fire Extinguisher -** Used on flammable liquids and flammable gasses.
129. **Class C Fire Extinguisher -** Used on electrical equipment.
130. **Class D Fire Extinguisher -** Used on combustible metals.
131. **Class K Fire Extinguisher -** Used on cooking oil and fat.
132. **Clean Power -** Pure, non-fluctuating, electrical power. SOURCE: Chapple, Stewart, & Gibson, 2018.
133. **Clipping Levels/Threshold -** Used in violation analysis. When a set value is surpassed, the event is recorded into an audit log. SOURCE: Chapple, Stewart, & Gibson, 2018.
134. **Cloud Computing -** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. SOURCE: CNSSI 4009-2015, p. 19.
135. **Code Review and Testing -** Used to identify bad programming patterns, security misconfigurations, functional bugs, and logic flaws.

136. **Cold Site** - A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. SOURCE: NIST SP 800-34, r1., p. G-1.
137. **Collision** - An event in which two different messages have the same message digest. SOURCE: NIST SP 800-106, p. 3.
138. **Collision Resistance** - An expected property of a cryptographic hash function whereby it is computationally infeasible to find a collision. SOURCE: NIST SP 800-106, p. 3.
139. **Compensating Security Controls** - The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system. SOURCE: NIST SP 800-137, p. B-2.
140. **Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)** - An interactive feature added to web forms to distinguish whether a human or automated agent is using the form. Typically, it requires entering text corresponding to a distorted image or a sound stream. SOURCE: NIST SP 800-63-3, p. 42.
141. **Common Criteria** - Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. SOURCE: NIST SP 800-53, r4., p. B-4.
142. **Compensative Control** - The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization. CNSSI 4009-2015, p. 23.
143. **Confidentiality** - Ensures unauthorized subjects are denied access to confidential objects and prevents authorized subjects from disclosure of protected data by preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and propriety information. SOURCE: NIST SP 800-152.
144. **Configuration Management** - A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. SOURCE: NIST SP 800-53, r4., p. B-4.

145. **Confusion** - Complicating the mapping between the plaintext and the encryption key, so an attacker cannot distinguish between the input and output processes. SOURCE: Pound, 2019.
146. **Continuity of Operations Plan (COOP)** - A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations. SOURCE: NIST SP 800-34 r1., p. G-1.
147. **Controlled Interface** - A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems. CNSSI 4009-2015, p. 32.
148. **Counter Mode (CTR)** - The DES encryption mode of a nonce + counter, then XOR'd with the corresponding message block, so each block is encrypted with a unique keystream. SOURCE: Pound, 2019.
149. **Countermeasure** - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards. SOURCE: NIST SP 800-137, p. B-5.
150. **Covert Channel** - An unintended or unauthorized intra-system channel that enables two cooperating entities to transfer information in a way that violates the system's security policy but does not exceed the entities' access authorizations. SOURCE: CNSSI 4009-2015, p. 33.
151. **Covert Storage Channel** - Involves the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. They typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels. SOURCE: NIST SP 800-53, r4., p. B-6.
152. **Covert Timing Channel** - A channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process. SOURCE: NIST SP 800-53, r4., p. B-6.
153. **Credential** - An object or data structure that authoritatively binds an identity via an identifier and additional attributes, to at least one authenticator possessed and controlled by a subject or subscriber. SOURCE: NIST SP 800-63-3, p. 44.
154. **Cross-site Request Forgery (CSRF**) - An attack in which a subject currently authenticated to a legitimate website and connected through a secure session browses to an attacker's website, causing subject's browser to be used to attack a vulnerable server. SOURCES: NIST SP 800-63-3, p. 44; Stewart, Chapple, & Gibson, 2018.

155. **Cross-site Scripting (XSS)** - A vulnerability that allows attackers to inject malicious code into an otherwise benign website. Often used with SQL script injection to redirect browsing to the attacker's website where confidentiality and integrity are compromised when the attacker transfers data between the website and the client, without the subject's knowledge. SOURCE: NIST SP 800-63-3, p. 44.
156. **Cryptanalysis** - Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. Also, the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security. This includes the process of looking for errors or weaknesses in the implementation of an algorithm or of the algorithm itself. SOURCE: CNSSI 4009-2015, p. 36.
157. **Cryptography** - 1. Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. SOURCE: CNSSI 4009-2015, p. 39.
158. **Cryptographic Hash Function** - A function that maps a bit string of arbitrary length to a fixed length bit string and is expected to have to be collision resistant, preimage resistant, and second preimage resistant. SOURCE: NIST SP 800-106, p. 3.
159. **Cryptographic Key** - A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. SOURCE: NIST SP 800-63-3, p. 44.
160. **Cryptographic Module** - A set of hardware, software, and or firmware that implements approved security functions (including cryptographic algorithms and key generation). SOURCE: NIST SP 800-63-3, p. 45.
161. **Data Custodian** - The individual tasked with assigning permissions to data and the daily maintenance and protection of data as assigned by upper management. SOURCE: Abernathy & McMillian; 2018; Chapple, Stewart, & Gibson, 2018.
162. **Data Encryption Standard (DES)** - The symmetric encryption algorithm defined as a 56-bit key algorithm developed by IBM in 1977, which the NSA proved as insecure. DES was replaced by AES in 2001. SOURCE: Pound, 2019; NIST SP 800-15.
163. **Data Loss Prevention (DLP)** - A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information. SOURCE: CNSSI 4009-2015, p. 39.

164. **Data Mining/Harvesting -** An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery. SOURCE: NIST SP 800-53, r4., p. B-6.
165. **Data Owner -** The person responsible to classify information and determine who may access data. SOURCE: Chapple, Stewart, & Gibson, 2018.
166. **Decoding/Decode -** Convert encoded data back to its original form of representation. SOURCE: CNSSI 4009-2015, p. 39.
167. **Defense in Depth -** Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. SOURCE: NIST SP 800-53, r4., p. B-6.
168. **Degauss -** To reduce the magnetic flux to virtual zero by applying a reverse magnetizing flied; demagnetizing media. SOURCE: CNSSI 4009-2015, p. 43.
169. **Demilitarized Zone (DMZ) -** Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. SOURCE: CNSSI 4009-2015, p. 43.
170. **Diffie-Hellman -** A common algorithm method of key exchange used to security exchange or establish secret keys (key materials) across an insecure network. It is used to create temporary or single-use secret keys. SOURCE: NIST SP 800-113.
171. **Diffusion -** Used to create randomness in the output of a ciphertext by making plaintext changes which carry throughout the ciphertext. SOURCE: Pound, 2019.
172. **Digital Certificate -** An electronic document often in X.509 format, containing the CA's digital signature and the owner's public key, by which they can be identified. SOURCE: Abernathy & McMillian, 2018.
173. **Digital Signature -** The result of a cryptographic transformation of data, that when properly implemented, provides the services of: 1. Origin authentication; 2. Data integrity, and 3. Signer non-repudiation. SOURCE: NIST SP 800-57, Pt1., r3.
174. **Digital Signature Algorithm (DSA) -** Used with digital signatures, it is a protocol based on algorithms similar to Diffie-Hellman and can be used with elliptic curve cryptography to increase the algorithm's strength. SOURCE: Pound, 2019.
175. **Disaster Recovery Plan (DRP) -** A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. NIST SP 800-37, r1., p. G-1.
176. **Discretionary Access Control (DAC) -** An access policy used to restrict access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g.,

users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control). SOURCE: NIST SP 800-53, r4., p. B-7.

177. **Disruption** - An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). SOURCE: NIST SP 800-34, r1., p. G-1.
178. **Domain** - An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. SOURCE: NIST SP 800-53, r4., p. B-7.
179. **Dry-Pipe Fire Extinguisher** - Pipes and sprinklers do not contain water but pressurized air. When a fire is detected, water is pumped into the pipes and sprinklers from a water storage holding tank usually located outside or below the facility.
180. **Electronic Code Book (ECB)** - The least secure, weakest, and most basic encryption mode. Based on a 64-bit block, it encrypts sequential blocks of data with one chosen secret key. The first block of data is encrypted into the next block to produce the ciphertext output, which can be identical to other produced blocks because the same key is used. SOURCES: Pound, 2019; Chapple, Stewart, & Gibson, 2018.
181. **Elliptic Curve Cryptography (ECC)** - A digital signature algorithm that is an analog of DSA using elliptic curve mathematics and speficied by ANSI standards. It can be used to replace Diffie-Hellman and DSA public key cryptography to perform modular arithmetic functions (y2 = x3 + ax + b). Elliptic Curve algorithms have shorter key sizes and are more efficient. SOURCES: NIST SP 800-57 Pt.1, r4; Pound, 2019.
182. **Encapsulating Security Payload (ESP)** - An IPsec security protocol that can provide encryption and or integrity protection for packet headers and data. SOURCE: NIST SP 800-77.
183. **Encryption** - The cryptographic transformation of data to produce ciphertext. SOURCE: CNSSI 4009-2015, p. 43.
184. **Endpoint Security/End-to-end security** - Safeguarding information in an information system from point of origin to point of destination. SOURCE: CNSSI 4009-2015, p. 47.
185. **Enterprise** - An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance of business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. SOURCE: NIST SP 800-53, r4., p. B-7.

186. **Ephemeral Mode** - Starting every session with a new key exchange to guarantee forward secrecy. SOURCE: Pound, 2019.
187. **Event** - Something that occurs within a system or network; an observable occurrence in an information system. SOURCES: NIST SP 800-92, p. A-1; 800-53, r4., p. B-7.
188. **Event Aggregation** - The consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event. SOURCE: NIST SP 800-92, p. A-1.
189. **Exclusive-Or (XOR)** - An encryption operation applied to two-bits. Two bits of the same value combine to produce the same results. Two bits with different values combine to the value of 1 (value can be A OR B, but not A AND B). SOURCE: Pound, 2019.
190. **Exfiltration** - The unauthorized transfer of information from an information system. SOURCE: NIST SP 800-53, r4., p. B-7.
191. **Extensible Authentication Protocol (EAP)** - Not a single protocol but a framework for port-based access control that uses the same three components as RADIUS. SOURCE: Abernathy & McMillian, 2018.
192. **Extranet** - A computer network that an organization uses for application data traffic between the organization and its business partners. SOURCE: CNSSI 4009-2015, p. 52.
193. **Fail Safe** - A mode of termination of system functions that prevents damage to specified system resources and system entities (e.g. specified data, property, and life) when a failure occurs or is detected in the system (but the failure still might cause a security compromise). SOURCE: CNSSI 4009-2015, p. 52.
194. **Fail Secure** - A mode of termination of system functions that prevents loss of secure state when a failure occurs or is detected in the system (but the failure still might cause damage to some system resource or system entity). SOURCE: CNSSI 4009-2015, p. 52.
195. **Failover** - The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system. SOURCE: NIST SP 800-53, r4., p. B-8.
196. **Fail Soft** - Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system. SOURCE: CNSSI 4009-2015, p. 52.
197. **False Acceptance Rate (FAR)** - Proportion of verification transaction with wrongful claims of identity that are incorrectly confirmed. Fail Soft - Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system. SOURCE: CNSSI 4009-2015, p. 52.
198. **False Rejection Rate (FRR)** - Proportion of verification transaction with truthful claims of identity that are incorrectly denied. Fail Soft - Selective termination of affected, non-essential system functions when a failure occurs or is detected in the system. SOURCE: CNSSI 4009-2015, p. 52.

199. **Fault** - A momentary electrical power outage.
200. **Feistel Cipher** - Uses hash functions in a series of permutations (transposition rounds) that can be reversed and converted into a block cipher. SOURCE: Pound, 2019.
201. Federal Information Security Management Act (FISMA) of 2002 - Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. SOURCE: CNSSI 4009-2015, p. 53.
202. **Fibre Channel over Ethernet (FCoE)** - A storage protocol that allows Fibre Channel frames to run at light speed on 10GB Ethernet networks. SOURCE: Abernathy & McMillian, 2018.
203. **Firewall** - A gateway that limits access between networks in accordance with local security policy. SOURCE: CNSSI 4009-2015, p. 54.
204. **Firmwar**e - Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. SOURCE: NIST SP 800-53, r4., p. B-8.
205. **Frequency Hopping Spread Spectrum (FHSS)** - Repeated switching of frequencies during radio transmission according to a specified algorithm, to minimize unauthorized interception or jamming of telecommunications. SOURCE: CNSSI 4009-2015, p. 55.
206. **Functional Testing** - Segment of quality assurance testing in which advertised security mechanism of an information system are tested against specification. SOURCE: CNSSI 4009-2015, p. 55.
207. **Gateway** - An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks. SOURCE: CNSSI 4009-2015, p. 55.
208. **Gray-box Testing** - Known also as focus testing, it is a test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. SOURCE: CNSSI 4009-2015, p. 55.
209. **Handshake** - Protocol dialogue between two systems for identifying and authenticating themselves to each other, or for synchronizing their operations with each other. SOURCE: IETF RFC 4949 v2.
210. **Hardware** - The physical components of an information system. SOURCE: NIST SP 800-53, r4., p. B-8.

211. **Hash** - a one-way function which maps strings of bits to fixed-length strings of bits, satisfying the properties that integrity is maintained if the sender's message digest value is compared and shown to be the same as the receiver's message digest value; and if the two MDs are different, modification has occurred and integrity has compromised. SOURCES: NIST SP 800-15; Abernathy & McMillian, 2018.
212. **Hash function** - Any size message is hashed to a fixed size output value (message digest). Hash functions are used with digital signatures, Message Authentication Codes (MACs) and even passwords to determine a shared key (e.g. Diffie-Hellman output). SOURCE: Pound, 2019.
213. **Hash Value** - The result of applying cryptographic hash functions to data (known also as a message digest). SOURCE: NIST SP 800-106, p.4.
214. **Hashed** - The process whereby data was input into a cryptographic hash function to produce a hash value. SOURCE: NIST SP 800-106, p. 4.
215. **Hashed Message Authentication Code (HMAC)** - A message authentication code that uses a cryptographic key in conjunction with a hash function. It is used to ensure message integrity through the use of a partial digital signature based on two keys and two applications of the hash function to solve attacks on SHA-1 AND SHA-2. Nonrepudiation is not guaranteed. SOURCES: NISTIR 7711, p. 68; Pound, 2019.
216. **Honeypot** - A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. SOURCE: CNSSI 4009-2015, p. 58.
217. **Hot Site** - A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption. SOURCE: NIST SP 800-34, r1., G-1.
218. **Hybrid/Hybrid Security Control** - A security control that is implemented in an information system in part as a common control and in part as a system-specific control. SOURCE: NIST SP 800-53, p. B-9
219. **Hypertext Transfer Protocol over TLS/SSL (HTTPS**) - The standard method for communication between clients and web servers, it is a secured version of HTTP using TLS/SSL and HTTP to secure website transaction; uses TCP port 443. SOURCE: NIST SP 800-101, r1., p.69.
220. **Identification** - The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. SOURCE: CNSSI 4009-2015, p.59.
221. **Incident** - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes,

stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. SOURCE: NIST SP 800-53, r4., p. B-9.

222. **Incident Response Plan** - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attacks against an organization's information system(s). SOURCE: NIST SP 800-34, r1., p. G-2.

223. **Industrial Control System (ICS)** - An information system used to control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. SOURCE: NIST SP 800-53, R4., p. B-9.

224. **Information assurance (IA)** - 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. SOURCE: CNSSI 4009-2015, p. 62.

225. **Information Owner/Data Owner** - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. SOURCE: NIST SP 800-137, p. B-6.

226. **Information Security Continuous Monitoring (ISCM**) - Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. SOURCE: CNSSI 4009-2015, p. 64.

227. **Information Security Officer (ISO)** - An executive or senior management person responsible for due care in performing risk analysis, mitigation, communicating risk to senior management, establishing security measures, and maintaining awareness of emerging threats. This individual recommends best practices to influence policies, standards, procedures, and guidelines to ensure the organization meets government and industry compliance. SOURCES: Abernathy & McMillian, 2018; Stewart, Chapple, & Gibson, 2015).

228. **Information System Owner** - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: NIST SP 800-53, r4., p. B-10.

229. **Initialization Vector (IV)** - A nonce that is associated with an invocation of authenticated encryption on a particular plaintext, used in defining the starting point of a cryptographic process. It is used to create randomness to increase the strength of encrypted data. The

IV may be randomly repeatable and should be unpredictable. SOURCES: NIST SP 800-38D, p.4; NIST SP 800-57, r4., p. 9.

230. **Insider Threat -** The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States or an organization. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. SOURCE: NIST SP 800-53, r4., p. B-12.

231. **Integrity -** Guarding against improper information modification or destruction by subjects, and includes ensuring information non-repudiation and authenticity. SOURCE: NIST SP 800-53, r4., p. B-12.

232. **Internet Control Message Protocol (ICMP) -** Protocol used for the exchange of control messages between hosts and gateways for diagnostics (e.g. ping, traceroute). Used by attackers for MiTM, DoS, and Ping of Death attacks. Security is enhanced when this protocol is blocked. SOURCE: Harris & Maymi, 2018.

233. **Internet Group Management Protocol (IGMP) -** A protocol used to manage multicasting groups or a set of hosts anywhere on a network that are interested in a particular multicast. Hosts send this protocol message to local agents to join and leave groups. SOURCE: Harris & Maymi, 2018.

234. **IP Security (IPsec) -** Operating at OSI network layer 3, this is a suite of protocols used to authenticate and or encrypt each IP packet in a data stream. Includes protocols for cryptographic key establishment used to secure connections between two devices and to protect traffic over a VPN. SOURCE: CNSSI-4009.

235. **Key -** A secret value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. When used, a message cannot be reversed without using the same bytes. In a database, a key is a database field, column or attribute. SOURCES: NIST SP 800-63-3; Chapple, Stewart, & Gibson, 2018.

236. **Key Escrow -** A deposit of the private key of a subscriber and other pertinent information based on the escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber’s private key for the benefit of the subscriber, an employer, or other party, based on the provisions set in the agreement, to ensure the subscriber will always have access to the private key should the vendor no longer be available. SOURCE: NIST SP 800-32, p. 49

237. **Key Exchange -** The process of two parties exchanging public keys in order to establish secure communications. SOURCE: NIST SP 800-32, p. 49

238. **Key Expansion -** Functions similar to a stream cipher where a fixed key length is generated into Round Keys that are used between rounds of a block cipher. SOURCE: Pound, 2019.
239. **Key Mixing -** The XOR function is applied to a key and message over encryption rounds to prevent a cipher from being reversed engineered. SOURCE: Pound, 2019.
240. **Key Pair -** Two mathematically related keys having where one key can be used to encrypt a message that can only be decrypted using the other key, and even knowing one key, it is computational infeasible to discover the other key. SOURCE: NIST SP 800-32, p. 49
241. **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. SOURCE: CNSSI 4009-2015, p. 76.
242. **Log -** A record of the events occurring within an organization's systems and networks. SOURCE: NIST SP 800-92, p. A-1.
243. **Log Analysis -** Studying log entries to identify events of interest or suppress log entries for insignificant events. SOURCE: NIST SP 800-92, p. A-1.
244. **Log Clearing -** Removing all entries from a log that precede a certain date and time. SOURCE: NIST SP 800-92, p. A-1.
245. **Log Management -** The process for generating, transmitting, storing, analyzing, and disposing of log data. SOURCE: NIST SP 800-92, p. A-1.
246. **Log Normalization -** Converting each log data field to a particular data representation and categorizing it consistently. SOURCE: NIST SP 800-92, p. A-1.
247. **Logic Bomb -** A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. SOURCE: CNSSI 4009-2015, p. 77.
248. **Logical Controls/Logical Access Controls -** An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database; it requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization. SOURCE: NIST SP 800-53, R4., p. B-13.
249. **Macro Viruses -** A virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate. SOURCE: CNSSI 4009-2015, p. 78.
250. **Maintenance Hook -** Code left behind in an application for developers to later access to fix the code; functions as a back door. Poses security risks as it may be exploited by an internal or external attacker.

251. **Malware/Malicious Code -** 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. Other examples include spyware and some forms of adware. SOURCE: NIST SP 800-53, r4., p. B-13.
252. **Mandatory Access Control (MAC) -** A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity; it is also a type of nondiscretionary access control. SOURCE: NIST SP 800-53, r4., p. B-14
253. **Maximum Tolerable Down Time (MTD) -** The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission. SOURCE: NIST SP 800-34, r1., p. G-2.
254. **Media -** Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. SOURCE: NIST SP 800-53, R4., p. B-14.
255. **Media Sanitization -** The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. SOURCE: CNSSI 4009-2015, p. 80.
256. **Memorandum of Agreement (MOA) -** A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes specific terms that are agreed to, and a commitment by at least one party to engage in action. It includes either a commitment of resources or binds a party to a specific action. SOURCE: CNSSI 4009-2015, p. 81.
257. **Memorandum of Understanding (MOU) -** A type of intra-agency, interagency, or National Guard agreement between two or more parties, which includes only general understandings between the parties. It neither includes a commitment of resources nor binds a party to a specific action. SOURCE: CNSSI 4009-2015, p. 81.
258. **Message Digest (MD) -** A digital signature that uniquely identifies data and has the property that changing a single bit in the data will cause a completely different message digest to be generated; used also in checksums to detect modification of data. SOURCE: NIST SP 800-92 p. A-2.
259. **Message Digest 2 (MD2) -** Ronald Rivest's 1989 secure hash for 8-bit processors, that produces a 128-bit hash with 18 rounds of computations. SOURCES: Stewart, Chapple, & Gibson, 2018; Abernathy & McMillian, 2018.

260. **Message Digest 4 (MD4)** - A message digest algorithm that produces a 128-bit hash value and performs only 3 rounds of computations. SOURCE: Abernathy & McMillian, 2018.
261. **Message Digest 5 (MD5)** - An unsecure 128-bit hash function that can be used as a checksum; it produces a 128-bit hash and performs 4 rounds of computations. SOURCES: Stewart, Chapple, & Gibson, 2018; Abernathy & McMillian, 2018.
262. **Message Digest 6 (MD6)** - A message digest algorithm that produces a variable hash value, performing a variable number of computations. SOURCE: Abernathy & McMillian, 2018.
263. **Message Authentication Code (MAC)** - A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data. Provides authenticity and integrity protection but lacks non-repudiation protection. SOURCES: NIST SP 800-63-3, p. 48.
264. **Message Authenticity** - Knowing a message or data is genuine, verified, and trusted with assurance the originator of the message possesses the same symmetric key. SOURCE: NISTIR 7298.
265. **Metadata** - Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels). SOURCE: NIST SP 800-53, r4., p. B-14.
266. **Mobile Code** - Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. SOURCE: NIST SP 800-53, r4., p. B-14.
267. **Mobile Device** - A portable computing device that can be easily be carried by a single individual; can operate without a physical connection (e.g., wirelessly transmit or receive information); has local, non-removable or removable data storage; and has a self-contained power source. Examples include smart phones, tablets, and E-readers. SOURCE: NIST SP 800-53, r4., p. B-14.
268. **Mode of Operation** - An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm, which can be used for message authentication. SOURCE: NISTIR 7298.
269. Multi-Factor Authentication - Authentication using two or more different factors to achieve authentication. Factors include: Type 1 - something you know (e.g., password/PIN); Type 2 - something you have (e.g., cryptographic identification device, token); or Type 3 - something you are (e.g., biometric). SOURCE: NIST SP 800-53, r4., p. B-14.

270. **Need to Know** - A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. SOURCE: CNSSI 4009-2015, p. 85.

271. **Network Administrator** - Ensures availability of the organization's network resources. Role should be separated from that of the Security Administrator role to avoid conflict of interests.

272. **Nonce** - Usually based on a time stamp, it is a string of bytes which never repeats and is used once in combination with a key to produce a random output every time; guards against replay attacks. SOURCES: NISTIR 7298; Stewart, Chapple, & Gibson, 2015.

273. **Non-Repudiation** - Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. SOURCE: NIST SP 800-53, r4., p. B-15.

274. **Objec**t - Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. SOURCE: NIST SP 800-53, r4., p. B-16.

275. **Object Identifier (OID)** - The unique alpha-numeric identifier registered under the ISO; it references a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported. SOURCE: NIST SP 800-32, p. 50.

276. **One-Time Pad (OTP)** - A manual substitution cipher produced in pad from and only used one time and every message has a different key. The encryption key is XOR'd with the corresponding plaintext and the key is the same length as the message. SOURCES: CNSSI-4009 & NISTIR 7298.

277. **One-Way Function/Algorithm** - Hash algorithms which map arbitrarily long inputs into a fixed-size output such that it is very difficult (computationally infeasible) to find two different hash inputs that produce the same output. Such algorithms are an essential part of the process of producing fixed- size digital signatures that can both authenticate the signer and provide for data integrity checking (detection of input modification after signature). SOURCE: CNSSI 4009-2015, p. 89.

278. **Open Shortest Path First (OSPF)** - A standards-based link state protocol, it is a routing protocol for IP networks. It uses link-state algorithms to calculate the shortest path between each node. SOURCE: Abernathy & McMillian, 2016.

279. **Outside Threat** - An unauthorized entity from outside the domain perimeter that has the potential to harm an information system through destruction, disclosure, modification of data, and or denial of service. SOURCE: NIST SP 800-32, p. 50.
280. **Padding** - Known also as traffic padding, it is mock bytes of data added to communications to both bring make a message meet a required block size and to disguise the size of actual data being transmitted. SOURCES: CNSSI-4009, NISTIR 7298; Pound, 2019.
281. **Passive Wiretapping** - The monitoring or recording of data that attempts only to observe a communication flow and gain knowledge of the data it contains, but does not alter or otherwise affect that flow. SOURCES: CNSSI-4009-2105, p. 91.
282. **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. SOURCE: NIST SP 800-53, r4., p. B-16.
283. **Personally Identifiable Information (PII)** - Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.). SOURCE: NIST SP 800-53, r4., p. B-16.
284. **Point-to-Point Protocol (PPP)** - A full-duplex TCP protocol used to connect two endpoints over a WLAN. In a wire WAN it uses a high-bandwidth fiver cable and the traffic is dedicated to the end points. Used also to connect non-LAN connections (e.g. modems, ISDN, VPNs, Frame Relay, and dial-up connections). Considered expensive. SOURCE: Chapple, Stewart, & Gibson, 2015.
285. **Point-to-Point Tunneling Protocol (PPTP)** - An enhanced version of PPP that uses generic routing encapsulation (GRE) to create encrypted tunnels between endpoints. Used with VPN and L2TP. Uses TCP port 1723. SOURCE: Chapple, Stewart, & Gibson, 2015.
286. **Portable Storage Device** - An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). SOURCE: NIST SP 800-53, r4., p. B-17.
287. **Primary Rate ISDN (PRI)** - A telecommunications solution that provides up to 23 B channels and a D channel for a total of 1.544 Mbps. SOURCE: Abernathy & McMillians, 2018.
288. **Private Encryption Key** - The key of a signature key pair used to create a digital signature; the key of an encryption key pair that is used to decrypt confidential

information. In both cases, this key must be kept secret. SOURCE: NIST SP 800-32, p. 50.

289. **Privileged Account -** An information system account with authorizations of a privileged user. SOURCE: NIST SP 800-53, r4., p. B-17.

290. **Public-key Cryptography -** Symmetric encryption where key pairs are used to encrypt and decrypt messages. Key pairs consist of one private key and one public key (published key). Two parties agree on a cryptographic algorithm to exchange keys. A digital signature can be verified by the corresponding private key. SOURCES: NIST SP 800-57 Part 1; NSTIR 7298; Pound, 2019.

291. **Public Key Infrastructure -** A set of policies, processes, server platforms, software, and workstations used for the purpose of administrating certificates and non-private key pairs, including the ability to issue, maintain, and revoke public key certificates. SOURCE: NIST SP 800-32, p. 51

292. **Random Bit -** A bit for which an attacker has exactly a 50% probability of success of guessing the value of the bit as either zero or one. SOURCE: NIST SP 800-106, p.4.

293. **Random Value -** A sufficient entropy bit string. SOURCE: NIST SP 800-106, p.4.

294. Randomized Hashing - A technique for randomizing the input to a cryptographic hash function. SOURCE: NIST SP 800-106, p.4.

295. **Reciprocal Agreement/Reciprocity -** Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. SOURCE: NIST SP 800-53, r4., p. B-18.

296. **Records -** The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended; known also as units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items). SOURCE: NIST SP 800-53, r4., p. B-18.

297. **Recovery Point Objective (PRO) -** The point in time to which data must be recovered after an outage. SOURCE: NIST SP 800-34 r1., p. G-2.

298. **Recovery Time Objective (RTO) -** The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes. SOURCE: NIST SP 800-34 r1., p. G-2.

299. **Reference Monitor -** A validation mechanism which as key component of an operating system, enforces an access control policy over all subjects and objects. It must always be invoked (i.e., complete mediation), tamperproof, and small enough to be subject to

analysis and tests, the completeness of which can be assured (i.e., verifiable). SOURCE: NIST SP 800-53, r4., p. B-18.

300. **Registration Authority** - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates, but is delegated certain tasks on behalf of an authorized CA. SOURCE: NIST SP 800-32, p. 51.

301. **Remanence** - Residual information remaining on storage media after clearing. See magnetic remanence and clearing. SOURCE: CNSSI 4009-2015, p. 102.

302. **Remote Access** - Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). SOURCE: NIST SP 800-53, r4., p. B-18.

303. **Remote Authentication Dial-In User Service (RADIUS)** - A networking protocol comprised of a supplicant, authenticator, and an authenticating server; used to manage users through authentication, authorization, and accounting (AAA). Used also by ISPs for backend 802.1x authentication. Runs in the OSI stack for email and client/server services. SOURCES: RFC 2138; Abernathy & McMillian, 2018.

304. **Repository** - Also known as a directory, it is a database containing information and data relating to certificates. SOURCE: NIST SP 800-32, p. 51.

305. **Residual Risk** - Portion of risk remaining after security measures have been applied. SOURCE: CNSSI 4009-2015, p. 103.

306. **Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability within a particular harmful result. SOURCE: NIST SP 800-32, p. 51.

307. **Risk Assessment** - The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. As part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. SOURCE: NIST SP 800-53, r4., p. B-19.

308. **Risk Management** - The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation. It includes establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time. SOURCE: NIST SP 800-53, r4., p. B-19.

309. **Risk Mitigation** - Prioritizing, evaluating, and implementing the appropriate risk- reducing controls/countermeasures recommended from the risk management process. SOURCE: NIST SP 800-53, r4., p. B-19.

310. **Risk Monitoring** - Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. SOURCE: NIST SP 800-53, r4., p. B-19.
311. **Risk Response** - Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. SOURCE: NIST SP 800-53, r4., p. B-19.
312. **Risk Tolerance** - The level of risk an entity is willing to assume in order to achieve a potential desired result. SOURCE: NIST SP 800-32, p. 51.
313. **Rivest, Shamir, and Adelman (RSA)** - Bearing its inventor's names, RSA is used for encryption and digital signing. RSA uses public-key cryptography based on factoring large prime numbers. SOURCE: Pound, 2019; Chapple, Stewart, & Gibson, 2015.
314. **Role-Based Access Control (RBAC)** - Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. SOURCE: NIST SP 800-53, r4., p. B-20.
315. **Safeguards** - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. SOURCE: NIST SP 800-53, r4., p. B-20.
316. **Salt/Salting** - A bit string generated during digital signature generation using the RSA Signature Scheme; when added to passwords it adds randomness to make the password unique. Adding salt can be done with Bcrypt and Password-Based Key Derivation Function 2 (PBKDF2). SOURCES: NIST SP 800-106, p.4.; Stewart, Chapple & Gibson, 2015.
317. **Sandboxing** - A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized. SOURCE: CNSSI 4009-2015, p. 106.
318. **Sanitization/Sanitize** - A process to render access to target data on the media infeasible for a given level of effort. Clear, purge, damage, and destruction are actions that can be taken to sanitize media. SOURCE: CNSSI 4009-2015, p. 106.
319. **Scoping Considerations** - A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the

security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective. SOURCE: NIST SP 800-53, r4., p. B-20.

320. **Secure Hash Standard -** Secure hash algorithms established by the government via the National Institute for Standards and Technology (NIST) for computing a condensed representation of electronic messages (data). There are multiple secure hash standards: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/244, and SHA-512/256. The secure hash algorithm is used to generate message digests. SOURCE: NISTIR 7298.

321. **Secure Shell (SSH) -** A protocol which allows users to remotely access systems using a secure end-to-end encryption. Often used with FTP, Telnet, and rlogin. Uses TCP port 22. SOURCE: Chapple, Stewart, & Gibson, 2015.

322. **Secure Socket Layer (SSL) -** An encryption protocol used as a TCP handshake to establish secure private communications during internet data transmissions. Usually presented in web browsers as “https.” SSL was established by Netscape. SOURCES: NISTIR 7298; Pound; Chapple, Stewart, & Gibson, 2015.

323. **Secure/Multipurpose Internet Mail Extensions (S/MIME) -** A set of specifications for securing electronic mail that is based upon the widely-used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer’s certificate(s). SOURCE: CNSSI 4009-2015, p. 107.

324. **Security Administrator -** Person responsible for all security related tasks to ensure confidentiality, integrity, and availability. This person performs due care by restricting access to objects and resources based on the principles of need to know and least privilege. Role should be separated from that of the Network Administrator to avoid conflict of interests.

325. **Security Assertion Markup Language (SAML) -** A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners. SOURCE: CNSSI 4009-2105, p. 108.

326. **Security Control -** A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its

information and to meet a set of defined security requirements. SOURCE: NIST SP 800-53, r4., p. B-21.

327. **Security Domain** - A domain that implements a security policy and is administered by a single authority. SOURCE: NIST SP 800-53, r4., p. B22.
328. **Security Information and Event Management (SIEM)** Software - A program that provides centralized logging capabilities for a variety of log types. SOURCE: NIST SP 800-92, p. A-1.
329. **Security Kernel** - Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct. SOURCE: NIST SP 800-53, r4., p. B23.
330. **Security Label** - The means used to associate a set of security attributes with a specific information object as part of the data structure for that object. SOURCE: NIST SP 800-53, r4., p. B23.
331. **Security Policy** - A set of criteria for the provision of security services. SOURCE: CNSSI 4009-2015, p. 111.
332. **Sensitive Information** - Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. SOURCE: NIST SP 800-53, r4., p. B23.
333. **Service Oriented Architecture (SOA)** - A set of principles and methodologies for designing and developing software in the form of interoperable services. These services are well-defined business functions that are built as software components (i.e., discrete pieces of code and/or data structures) that can be reused for different purposes. SOURCE: NIST SP 800-53, r4., p. B-23.
334. **Session Initiated Protocol (SIP)** - A signaling protocol used to manage multimedia connections (e.g., voice, video, IP networks) while providing integrity.
335. **SHA-1** - A 160-bit block size (output) secure hash standard prone to collisions but can be safely used by HMAC. It was replaced by SHA-2. SOURCE: Pound, 2019.
336. **SHA-2** - Producing a 256 or 512-bit block message digest, SHA-2 decreases collisions and is generally considered secure. It can be used for digital signatures, key-hash message authentication codes, random number generation, and with other cryptographic algorithms. SOURCES: NISTIR 7298; Pound, 2019.
337. **SHA-3** - Known also as the Keccak algorithm, SHA-3 functions differently than SHA-1 and SHA-2. It is currently being developed as an alternative to SHA-2 in the event SHA-2 is found to be unsecure. SOURCES: Pound, 2019; Chapple, Stewart, & Gibson, 2015.

338. **Simple Mail Transfer Protocol (SMTP)** - A protocol for email transmission; uses TCP Port 25.

339. **Simple Network Management Protocol (SNMP) -** An application layer protocol requiring minimal software that is a standard internet protocol used for network monitoring. It is used to retrieve information from network devices and to send configuration changes to those devices. Uses TCP port 161. SOURCE: Abernathy & McMillan, 2018.

340. **Software -** Computer programs and associated data that may be dynamically written or modified during execution. SOURCE: NIST SP 800-53, r4., p. B-23.

341. **SP-Network -** An encryption method that chains substitution and permutation operations to each other in a block cipher structure. SOURCE: Pound, 2019.

342. **Spywar**e **-** Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. SOURCE: NIST SP 800-53, r4., p. B-24.

343. **Stream Cipher -** An encryption algorithm that generates a pseudorandom keystream (sequence of symbols or their electrical or mechanical equivalents), by XORing each part of the key with the corresponding plaintext. Stream Ciphers operated on one bit at a time. SOURCES: CNSSI-4009; Pound, 2019; Chapple, Stewart, & Gibson, 2015.

344. **Supply Chain -** Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer. SOURCE: NIST SP 800-53, r4., p. B24.

345. **Symmetric Encryption -** Known also as symmetric encryption algorithm, it is encryption that uses the same, single key for the process of encryption and decryption. SOURCE: CNSSI-4009.

346. **Synchronous Crypto-operation -** Method of on-line cryptographic operation in which cryptographic equipment and associated terminals have timing systems to keep them in step. SOURCE: CNSSI 4009-2015, p. 119.

347. **Syslog -** A protocol that specifies a general log entry format and a log entry transport mechanism. SOURCE: NIST SP 800-92, p. A-2.

348. **System Development Life Cycle (SDLC) -** The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. SOURCE: NIST SP 800-34, r1, p. G-3.

349. **System Owner -** Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. SOURCE: CNSSI 4009-2015, p. 120.

350. **TACACS+** - A Cisco proprietary authentication service that supports centralized authentication services such as RADIUS, Telnet, rlogin, PPP, SLIP, or EXEC services. SOURCE: Benjamin, 2005.
351. **Tactical Plans** - An organization's short term plans covering a six month to a year, with details on how to implement the strategic plan.
352. **Tailoring** - The process to modify security control baselines by identifying and designating common controls; Applying scoping to the applicability and implementation of baseline controls; Selecting compensating security controls; Assigning specific values to organization-defined security control parameters; Supplementing baselines with additional security controls or control enhancements; and providing additional specification information for control implementation. SOURCE: NIST SP 800-53, r4., p. B-25.
353. **Tangible Assets** - All resources that can by physically touched, e.g. equipment, personnel, facilities.
354. **Teardrop Attack** - A DoS attack that causes a buffer-overflow and a system crash due to fragmented packets being reassembled.
355. **Telne**t - The abbreviate name for teletype network, it is a protocol that uses a command line to access another host. As it does not provide encryption, the protocol poses serious security risks as it can be used by attackers to install malware or viruses on a targeted system, or to extract sensitive information. Uses TCP port 23. SOURCE: RFC 855.
356. **Threat** - Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and or denial of service. SOURCE: NIST SP 800-32, p. 51.
357. **Threat Agent/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. Synonymous with threat agent. SOURCE: NIST SP 800-53, r4., p. B25.
358. **Three-legged Firewall** - A firewall with three interfaces allowing the addition of a DMZ; it requires the firewall to be configured to route packets between the outside world and the DMZ differently than between the outside world and the internal network (one interface towards the internal network, one to the DMZ, and one to the internet). SOURCE: Firewall.CX, 2019.
359. **Tiger** - A very fast hash function used on 64-bit processors and produces hashes with bit values of 128-, 160-, or 192-bits. It performs 24 rounds of computations on 512-bit blocks.
360. **Time Division Multiplexing (TMD)** - A method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration. Each individual data stream is reassembled at the receiving end based on the timing. SOURCE: Rouse, 2019.

361. **Time of Check/Time of Use (TOC/TOC) -** A timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request. SOURCE: Chapple, Stewart, & Gibson, 2015.
362. **Total Risk -** The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). SOURCE: NIST SP 800-16.
363. **Trade Secret -** Any valuable commercial information or intellectual property that provides a business with an advantage over competitors who do not have that information. Examples include recipes, formulas, ingredient listings, and other information that must be protected against disclosure. SOURCE: The Free Dictionary; Abernathy & McMillian, 2018.
364. **Trademark -** A registered word, slogan, or logo used to identify a company and its products or services. SOURCE: Chapple, Stewart, & Gibson, 2015.
365. **Transport Layer (Layer 4) -** OSI layer that receives data from layers 7, 6, and 5 OSI, which then adds information to identify the transport protocol and port numbers in use at layer 7. SOURCE: Abernathy & McMillian, 2018.
366. **Transport Layer Security/Secure Sockets Layer (TLS/SSL) -** A security protocol providing privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. CNSSI 4009-2015, p. 125.
367. **Transmission Control Protocol (TCP) -** A reliable, error-free, connection-oriented transmission that uses a three-way handshake to establish communications (SYN, SY/ACK, ACK); it uses well-known ports 0-1023. It enables two hosts to establish a connection and exchange streams of data with a guarantee that transmitted packets will be delivered in the same order in which they were sent. SOURCE: NIST SP 800-82, r2., p. B-17.
368. **Transport Layer Security (TLS) -** The current replacement for Secure Socket Layer (SSL), also known as SSL 3 or TLS 1. TLS uses TCP port 443. SOURCE: Pound, 2019; Chapple, Stewart, & Gibson, 2015.
369. **Transposition cipher** - Cipher that uses an encryption algorithm to rearrange the letters of a plaintext message to form the ciphertext message. SOURCE: Chapple, Stewart, & Gibson, 2015.
370. **Trapdoor -** A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data. See backdoor. Also, in cryptography, one-to-one function that is easy to compute in one

direction, yet believed to be difficult to invert without special information. SOURCE: CNSSI 4009-2015, p. 126.

371. **Triple DES (3DES) -** An implementation of the data encryption standard (DES) algorithm that uses three passes of the DES algorithm instead of one as used in ordinary DES applications. Triple DES provides much stronger encryption than ordinary DES but it is less secure than advanced encryption standard (AES). SOURCE: CNSSI 4009-2015, p. 126.
372. **Trojan horse -** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. SOURCE: CNSSI 4009-2015, p. 126.
373. **Trusted Agent -** Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. They do not have automated interfaces with Certification Authorities. SOURCE: NIST SP 800-32, p. 51.
374. **Trusted Certificate -** A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Known also as “trust anchor.” SOURCE: NIST SP 800-32, p. 51.
375. **Trusted Computer Base (TCB) -** Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy. SOURCE: CNSSI 4009-2015, p. 127.
376. **Trusted Path -** A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software. SOURCE: NIST SP 800-53, R4., p. B25.
377. **Trusted Platform Module (TMP) -** A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys. SOURCE: NIST SP 800-147, p. B-1.
378. **Trusted Recovery -** Ability to ensure recovery without compromise after a system failure. SOURCE: CNSSI 4009-2015, p. 127.
379. **Trusted Third-Party Federated Identity Model -** A federated identity model in which each organization subscribes to the standards of a third party. SOURCE: Abernathy & McMillian, 2018.

380. **Tumbler Lock** - A cylinder type lock operated with a key use tumbler pins, wafers, wards, or levers, to control the lock's operation. Movable pins prevent the lock from opening unless a key correctly rotates the pins into position to open the lock.
381. **Twisted Pair** - Two independently insulated, thin diameter, copper wires that are twisted loosely around each other to prevent cross-talk and electromagnetic interference. Typically terminated with an RJ45 connector and used with 10BaseT, it is the Ethernet wiring standard for 10 Mbps for distances of up to 100 meters. SOURCE: LINFO, 2005.
382. **Two-Person Control** - The continuous surveillance and control of material at all times by a minimum of two authorized individuals, each capable of detecting incorrect or unauthorized procedures with respect to the task being performed and each familiar with established security requirements. SOURCE: CNSSI 4009-2015, p. 127.
383. **Twofish** - A 1998 block cipher by Counterpane Labs, that has a 128-bit block size, a key size ranging from 128 to 256 bits, and is optimized for 32-bit CPUs; there is no current successful cryptanalysis of twofish. SOURCE: Schneier, 2019.
384. **Unicast** - A one-to-one transmission between systems.
385. **Uninterruptible Power Supply (UPS)** - A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost. It should be located between the wall outlet and the electronic device. SOURCES: NISTIR 7621, r.1, p. 18; Abernathy & McMillan, 2018.
386. **United States Sentencing Guidelines of 1991** - Legislation which established sentencing policies and practices for the federal criminal justice system for individual and organizations convicted of federal crimes such as Class A misdemeanors. SOURCE: U.S. Sentencing Commission, 2019.
387. **URL Hiding** - An attack that takes advantage of the ability to embed URLs in web pages and email. SOURCE: Abernathy & McMillan, 2018.
388. **US PATRIOT ACT of 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)** - Legislation enacted after September 11, 2001, which increased law enforcement and intelligence agencies to conduct monitoring and other activities of suspected terrorists. SOURCE: U.S. DOJ, 2019.
389. **User** - Individual, or (system) process acting on behalf of an individual, authorized to access an information system. SOURCE: NIST SP 800-53, r4., p. B26.
390. **Verification** - Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. May also be the process of confirming or denying identification claimed by a subject based on comparing authentication factors of the person requesting access to an object or resources. SOURCE: NIST SP 800-161.

391. **Very High Bit-Rate DSL (VDSL) -** An advanced version of DSL broadband internet, with downloads of up to 52 Mbps. SOURCE: Frontier, 2019.
392. **View -** A client interface used to interact with a database to limit what a subject can see and do with the database. SOURCE: Chapple, Stewart, & Gibson, 2015.
393. **Virtual LAN (VLAN) -** A logical network segmentation implemented on switches and bridges to manage traffic. When multiples are used on a single switch, they are considered separate physical networks and function as such. SOURCE: Chapple, Stewart, & Gibson, 2015.
394. **Virtual Private Network (VPN) -** Protected information system link utilizing tunneling, security controls, and endpoint address translation viging the impression of a dedicated line. SOURCE: NIST SP 800-53, r.4.
395. **Virtual Storage Area Network (VSAN) -** A collection of ports from the set of connected Fibre Channel Switches (FCS) used to form to increase storage scalability within a network. SOURCE: Sibergen, 2019.
396. **Virus -** A computer program containing a malicious segment that attaches itself to an application of program or another executable component. SOURCE: NIST SP 800-47.
397. **Vishing -** Phishing which targets Voice over IP systems by spoofing the caller's number to evade caller ID. SOURCE: Chapple, Stewart, & Gibson, 2015.
398. **Volatile Memory -** Memory that loses its content when power is turned off or lost. SOURCE: NIST SP 800-72, p.59.
399. **V-Shaped Model -** A development model which plans steps in a V format to emphasize the formal verification and validation at each step of the product's development. SOURCE: Harris & Maymi, 2018.
400. **Vulnerability -** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: NIST SP 800-53, r4., p. B-25.
401. **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. SOURCE: NIST SP 800-53, r4., p. B25.
402. **War Chalking -** Used in the late 1990's a type of graffiti used between cybersecurity attackers to inform each other of unprotected wireless networks in an area.
403. **War Driving -** Used by attacker to search out access point radio signals to unprotected wireless networks.

404. **Warded Lock** - A lock with obstructions that will not open unless a key with corresponding notches is used.
405. **Warm Site** - A leased or rented facility partially equipped with configured equipment and includes utilities but not computer equipment. SOURCE: Harris & Maymi, 2018.
406. **Waterfall Model** - Development model that uses a linear-sequential life-cycle approach, where each stage must be fully completed before the next stage can begin. SOURCE: Harris & Maymi, 2018.
407. **Wave Motion Detector** - Known also as a microwave motion sensor, it emits waves which are then reflected back to the device receiver to detect moving objects.
408. **Web Application Security Consortium (WASC)** - A 501c3 nonprofit made up of an international group of experts, industry practitioners, and organizational representatives who produce open source and widely agreed upon best-practice security standards for the World Wide Web.
409. **Wet Pip Fire Extinguisher** - A fire extinguisher system in which water is constantly maintained within the sprinkler piping. When a sprinkler activates this water is immediately discharged onto the fire (not optional for rooms with electrical equipment). SOURCE: VFP Fire Systems, 2019.
410. **Whaling** - A specific kind of phishing that targets high-ranking members of organizations. SOURCE: CNSSI 4009-2015, p. 132.
411. **White Box Testing** - A test method that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. SOURCE: NIST SP 800-53A, r4.
412. **Whitelisting** - The process used to identify software programs that are authorized to execute on an information system, or authorized URLs and websites. SOURCE: NIST SP 800-53, r4., p. B26.
413. **Wide Area Network (WAN)** - A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN. SOURCE: NIST SP 800-82, r2., p. B-18.
414. **Wi-Fi Protected Access 2 (WPA2)** - The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For federal government use, the implementation must use federal information processing standards (FIPS) approved encryption, such as advanced encryption standard (AES). SOURCE: CNSSI 4009, p. 132.
415. **Wired Equivalent Privacy (WEP)** - A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Weaknesses have been found in

it and so that it is no longer considered a viable encryption mechanism. SOURCE: NIST SP 800-48, r1., p. B-1.

416. **Wireless Local Area Network (WLAN)** - A group of wireless APs and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility. SOURCE: NIST SP 800-48, r1., p. B-1.
417. **Work Factor** - Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure. SOURCES: CSRC; CNSSI 4009, p. 133.
418. **Worm** - A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. SOURCE: NIST SP 800-82, r2.
419. **WPA2** - The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For federal government use, the implementation must use federal information processing standards (FIPS) approved encryption, such as advanced encryption standard (AES). SOURCE: CSRC, under WPA2.
420. **X.25** - The ITU-T standard that defines how connections between DTE and DCE are maintained for remote terminal access and computer communications in PDNs. It specifies LAPB, a data link layer protocol, and PLP, a network layer protocol. Frame Relay has to some degree superseded this protocol. SOURCE: Cisco, 2019.
421. **Zachman Framework** - A schema used in software development processes in which questions (what, how, when, who, where, and why) are intersected with answers related to identification, definition, representation, specification, configuration, and instantiation. SOURCE: Zachman, 2019.
422. **Zero Day Attack** - An attack that exploits a previously unknown hardware, firmware, or software vulnerability. SOURCE: CNSSI 4009-2015, p. 133.
423. **Zero-knowledge Proof** - Allows a claimant to be authenticated to a Verifier without revealing the encryption key, password, or other information to the Verifier. SOURCE: NIST SP 800-63-3.

REFERENCES

(n.d.). Border Gateway Protocol (BGP). *Cisco*. Retrieved from: https://www.cisco.com/c/en/us/products/ios-nx-os-software/border-gateway-protocol-bgp/index.html

Ibid., (n.d.). X.25 Protocol. *Cisco.* Retrieved June 16, 2019 from: https://www.cisco.com/c/en/us/tech/wan/x-25-protocols/index.html

(n.d.). Glossary, Computer Security Resource Center (CSRC). *Recommendations from the Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST).* Retrieved from: https://csrc.nist.gov/Glossary

(1983, May). RFC 855, Telnet Option Specifications. *Working Group. Recommendations from the Internet Engineering Task Force (ITEF).* Retrieved from: https://tools.ietf.org/html/rfc855

(1991). Federal Sentencing Guidelines Manual. *U.S. Sentencing Commission.* Retrieved June 16, 2019 from: https://www.ussc.gov/guidelines/archive/1991-federal-sentencing-guidelines-manual

(1997, April). RFC 2138, Remote Authentication Dial In User Service (RADIUS). *Network Working Group. Recommendations from the Internet Engineering Task Force (ITEF).* Retrieved from: https://www.ietf.org/rfc/rfc2138.txt

(2001, November). Federal Information Processing Standards Publication (FIPS) 197, Announcing the Advance Encryption Standard (AES*). Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

(2005). Twisted Pair Definition. *The Linux Information Project (LINFO).* Retrieved June 16, 2019 from: http://www.linfo.org/twisted_pair.html

(2006, March). Federal Information Processing Standards Publications (FIPS) 200, Minimum security requirements for federal information and information systems.

Recommendations from the National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

(2011, March). NIST SP 800-39, Managing information security risk, organization, mission, and information system view. Joint Task Force Transformative Initiative. Computer Security Division, ITL, NIST, Gaithersubre, MD. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

(2012, March 16). IEEE 828, Standard for Configuration Management in Systems and Software Engineering. *Recommendations from the IEEE.* Retrieved June 14, 2019 from: https://standards.ieee.org/standard/828-2012.html

(2013, April). NIST, SP 800-53, Rev.4, Security and privacy controls for federal information systems and organizations. *Recommendations from the Joint Task Force Transformation Initiative* and the *National Institute of Standards and Technology.* Retrieved from: http://dx.doi.org/10.6028/NIST.SP.800-53r4

(2019). Online dictionary. *Merriam-Webster, Inc.* Retrieved from: https://www.merriam-webster.com/dictionary/attenuation

(2019). Trade Secret. *The Free Legal Dictionary.* Retrieved on June 16, 2019 from: https://legal-dictionary.thefreedictionary.com/trade+secret

(2019). Three-legged firewall, Firewall Topologies. *Firewall.CX.* Retrieved on June 16, 2019 from: http://www.firewall.cx/networking-topics/firewalls/209-firewall-topologies.html

(2019). The USA PATRIOT Act: Preserving Life and Liberty. *The U.S. Department of Justice.* Retrieved June 16, 2019, from: https://www.justice.gov/archive/ll/highlights.htm

(2019). What is VDSL? The Connection. *Frontier Communications, Inc*. Retrieved June 16, 2019, from: https://internet.frontier.com/resources/resources/dsl-demystified/what-is-vdsl/

(2019). What is vSAN technology and why do you need it? Sibergen Technologies. Retrieved June 16, 2019, from: https://sibergen.com/vsan-technology-need/

(2019). Wet Pipe Fire Sprinkler System. VFP Fire Systems. Retrieved June 16, 2019 from: https://www.vfpfire.com/systems-wet-pipe.php

Abernathy, R. & McMillan, T. (2018). CISSP Cert Guide, 3rd Edition, Glossary, pp.613-669. *Pearson Education,* Indianapolis, Indiana.

Ayers, R., Brothers, S., & Jansen, W. (2014, May). NIST SP 800-101, Rev.1, Guidelines on mobile device forensics. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Bader, L., Souppaya, M., Trapnell, M., Trapnell, E., Yaga, D., & Scarfone, K. (2016, December). NIST SP 800-179, Guide to securing Apple OS X10.10 systems for IT professionals: an NIST security configuration checklist. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-179.pdf

Bakiciol, T., Cojacaru-Durand, N., & Lu, D. (n.d.). Basel II. Princeton University. Retrieved from: https://www.princeton.edu/~markus/teaching/Eco467/10Lecture/Basel2_last.pdf

Barker, E. (2016, January). Recommendation for Key Management, NIST SP 800-57 Pt.1, Rev. 4. *Recommendations from the National Institute of Standards and Technology*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

Barker, E., & Kelsy, J. (2015, June). NIST SP 800-90A Rev.1, Recommendation for random number generation using deterministic random bit generators. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

Benjamin, H. (2005, October 28). Terminal Access Controller Access Control System Plus (TACACS+). CCIE Self-Study: Security Protocols. *Cisco Press.* Retrieved on June 16, 2019 from: http://www.ciscopress.com/articles/article.asp?p=422947&seqNum=4

Boyens, J. Paulsen, C., Moorthy, R., & Bartol, N. (2015, April). NIST SP 800-61, Supply chain risk management practices for federal information systems and organizations. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: http://dx.doi.org/10.6028/NIST.SP.800-161

Brewer, D., & Nash, M. (1989). The Chinese wall security policy. Gamma Secure Systems Limited. Glenhurst close, Blackwater, Camberley, Surry, GU17 9BQ, UK. Retrieved from Purdue University: https://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/brewer_nash_89.pdf

Chapple, M., Stewart, J.M., & Gibson, D. (2018). Glossary for the CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, Eigth Edition. [Apple iBooks]. Sybex. *John Wiley & Sons, Inc.,* Indianapolis, Indiana.

Cooper, D., Polk, W., Regenscheid, A., & Souppaya, M. (2011, April). NIST SP 800-147, BIOS protection guidelines. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-147.pdf

Dang, Q. (2009, February). NIST SP 800-106, Randomized hashing for digital signatures. Computer Security Division, Information Technology Laboratory. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-106.pdf

Dang, Q. (2012, August). NIST SP 800-107, Rev. 1,Recommendation for applications using approved hash algorithms. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf

Dempsey, K., Eavy, P., & Moore, G. (2017, June). NISTIR 8011 Vol. 1, Automation support for security control assessments, Vol. 1: overview. *Recommendations of the National Institute of Standards and Technology*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf

Dempsey, K., Chawal, N., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011, September). NIST SP 800-137, Information security continuous monitoring (ISCM) for federal information systems and organizations. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

Doraiswamy, A. (2011, October 25). Blind SQL Injection 1.0 - attack anatomy. INFOSEC. Retrieved June 14, 2019, from: https://resources.infosecinstitute.com/blind-sql-injection/

Dukes, C. (2015, April). Committee on National Security Systems (CNSSI) No. 4009. Retrieved from https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Dworkin, M. (2007, November). NIST SP 800-38D, Recommendation for block cipher modes of operations: Galois/Counter Mode (GCM) and GMAC. Computer Security Division, Information Technology Laboratory. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

Frankle, S., Hoffman, P., Orebaugh, A., & Park, R. (2008, July). NIST SP 800-113, Guide to SSL VPNs. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf

Freeman, Z. (2014). SQL: What is a base relation? Quora. Retrieved June 14, 2019 from: https://www.quora.com/SQL-What-is-a-base-relation

Grassi, P., Garcia, M., & Fenton, J. (2017, June). NIST SP 800-63-3, Digital identity guidelines. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://doi.org/10.6028/NIST.SP.800-63-3

Harris, S., & Maymi, F. (2018). All in One CISSP Exam Guide, 8th Ed., Apple iBook conversion by Code Mantra. *McGraw Hill Education.* New York, NY.

Hu, C., Ferraiolo, D., & Kuhn, D. (2006, Sept.). NISTIR 7316 Assessment of Access Controls. *Recommendations of the National Institute of Standards and Technology*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf

Hu., C., Kuhn, R., & Yaga, D. (2017, June). NIST SP 800-192, Verification and test methods for access control policies/models. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-192.pdf

Jansen, W., & Ayers, R. (2004, November). NIST SP 800-72, Guidelines on PDA Forensics. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-72.pdf

Kent, K., & Souppaya, M. (2006, Sept.). NIST-SP 800-92, Guide to Computer Security Log Management. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

Kissel, R. (2013, May). Glossary of Key Information Security Terms, NSTIR 7298, Rev.2. *U.S. Department of Commerce, National Institute of Standards and Technology.* Retrieved from: https://doi.org/10.6028/NIST.IR.7298r2

Kuhn, D., Hu, V., Polk., W., & Chang, S. (2001, February). NIST SP 800-32, Introduction to public key technology and the federal PKI infrastructure. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf

Miessler, D. (2014, June 28). The Birthday Attack. Daniel Miessler, online. Retrieved from: https://danielmiessler.com/study/birthday_attack/

Niele, M., Dempsy, K., Pillitteri, V. (2017, June). NIST SP 800-12, An Introduction to Information Security. NIST SP 800-12, Rev.1. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://doi.org/10.6028/NIST.SP.800-12r1.

Norton. (2019). What is a botnet? Malware. Norton by Symantec. Retrieved from: https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

Padgette, J., Bahr, J., Holtmann, M. Smithbey, R., & Scarfone, K. (2017, May). NIST SP 800-121 Rev. 2, Guide to Bluetooth security. Recommendations of the National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

Paulsen, C., & Toth, P. (2016, November). NISTIR 7621, R1, Small business information security: the fundamentals. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://doi.org/10.6028/NIST.IR.7621r1

Pound, M. (2019), Encryption Glossary, Version 1.5. O'Reilly Online Training, Introduction to Encryption. Retrieved June 8, 2019 from: https://cryptography.io/en/latest/glossary/

Regenscheid, A., & Beier, G. (2011, September). NISTIR 7711, Security best practices for the electronic transmission of election materials for UOCAVA voters. Information Technology Laboratory. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7711.pdf

Ross, R., McEvilley, M., & Oren, J.C., (November, 2016). NIST SP 800-160, Systems Security Engineering, Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. *Recommendations of the National Institute of Standards and Technology*. Retrieved from: https://doi.org/10.6028/NIST.SP.800-160

Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2016, December). NIST SP 800-171, Rev.1, Protecting controlled unclassified information in nonfederal systems and organizations. *Recommendations of the National Institute of Standards and Technology.* Retrieved from: https://doi.org/10.6028/NIST.SP.800-171r1

Ross, R., Swanson, M., Katzke, S., & Johnson, A. (2004, May). NIST SP 800-37 Rev.1, Guide for the security certification and accreditation of federal information systems. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-37.pdf

Rouse, M. (2019). Time-division multiplexing (TMD). *TechTarget.* Retrieved on June 16, 2019 from: https://whatis.techtarget.com/definition/time-division-multiplexing-TDM

Scheier, B. (2019). The Blowfish encryption algorithm. *Schneier on Security.* Retrieved June 14, 2019, from: https://www.schneier.com/academic/blowfish/

Ibid., (2019). Twofish. *Schneier on Security.* Retrieved June 14, 2019, from: https://www.schneier.com/academic/twofish/

Shirey, R., (2007, August). IETF RFC 2828. Internet Security Glossary. *Working Group. Internet Engineering Task Force (IETF).* Retrieved from: https://www.rfc-editor.org/info/rfc2828

Stoneburner, G., Hayden, C. and Feringa, A. (2004, June). NIST SP 800-27 Rev A., Engineering Principles for Information Technology Security (A Baseline for Achieving Security). *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015, May). NIST SP 800-82, Guide to Industrial Control Systems (ICS). *Recommendations from the National Institute of Standards and Technology.* Retrieved from: http://dx.doi.org/10.6028/NIST.SP.800-82r2

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010, May). NIST SP 800-34 R1., Contingency planning guide for federal information systems. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Symanovich, S. (2019). What is a privacy breach? *Norton by Symantec*. Retrieved June 14, 2019 from: https://us.norton.com/internetsecurity-privacy-what-is-a-privacy-breach.html

Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (2007, February). NIST SP 800-45 v.2, Guidelines on electronic mail security. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf

Wison, M., Zafra, D., Pitcher, S., Tressler, J., & Ippolito, J. (1998, April). NIST SP 800-16, Information Technology Security Training Requirements: A role- and performance-based mode. *Recommendations from the National Institute of Standards and Technology.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Zachman, J. (2019). The concise definition of The Zachman Framework by John A. Zachman. *Zachman International.* Retrieved June 16, 2019 from: https://www.zachman.com/about-the-zachman-framework