METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 2
SUBJECT: METROPOLITAN GOVERNMENT INFORMATION SECURITY GLOSSARY	DISTRIBUTION DATE: 10/8/2010
	EFFECTIVE DATE: IMMEDIATELY
ISSUING AUTHORITY: Director of Information Technology Services of the Metropolitan Government of Nashville and Davidson County	EXPIRATION: UNTIL RESCINDED

PURPOSE

Metropolitan Government has implemented an Information Security Management program per Executive Order No. 038. A core component of this program is a set of information security policies based on international standards. This document provides specific definitions for information security terminology used in Metropolitan Government's information security policies.

CONTENT

The glossary was created initially with those terms deemed common to the Metropolitan Government Information Security Management program policies, plans, and other documents. The definitions are taken from a variety of industry standard sources, as indicated at the end of each definition.

As policies and plans are developed by work groups, new definitions may be added. These definitions may also come from industry standard sources, or may be fashioned by the work group, for which the work group is credited as the source at the end of the definition.

Definitions added by work groups are voted on for inclusion to this document by the Information Security Steering Committee.

GLOSSARY

Access –Ability to make use of any information system (IS) resource. SOURCE: SP 800-32 Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. SOURCE: CNSSI-4009

Access Agreement – Confidentiality, business associate and non-disclosure agreements are a form of access agreement. Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Access agreements shall include an acknowledgement that individuals have read, understand and agree to abide by the constraints associated with the information system to which access is authorized. SOURCE: Confidentiality Agreements Work Group; SP 800-53

Access Control – The process of granting or denying specific requests to: 1) obtain and use information

and related information processing services; and 2) enter specific physical facilities (e.g., city buildings). SOURCE: FIPS 201; CNSSI-4009

Access Control Mechanism – Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. SOURCE: CNSSI-4009

Account Management, User – Involves 1) the process of requesting, establishing, issuing, and closing user accounts; 2) tracking users and their respective access authorizations; and 3) managing these functions. SOURCE: SP 800-12

Accountability – Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information. SOURCE: CNSSI-4009

Acknowledgement - A declaration or avowal of user's own act, to give it legal validity. SOURCE: Confidentiality Agreements Work Group

Administrative Safeguards – Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information. SOURCE: SP 800-66

Advisory – Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems. SOURCE: CNSSI-4009

Affiliates – Any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides data processing services. SOURCE: Metro Government Legal Department

Agency – An agency of the Metropolitan Government.

Alert – Notification that a specific attack has been directed at an organization's information systems. SOURCE: CNSSI-4009

Alternate Work Site – Organization-wide, program allowing employees to work at home or at geographically convenient satellite offices for part of the work week (e.g., telecommuting). SOURCE: CNSSI-4009

Antivirus Software – A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. SOURCE: SP 800-83

Antivirus Signatures - A catalog of data that describes the current Malicious Software threats (e.g., virus, worms, spyware) and how Antivirus Software is to detect and remove the threat from the given system, message or file. SOURCE: SP 800-83

Application – The use of information resources (information and information technology) to satisfy a specific set of user requirements. SOURCE: SP 800-37 Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. SOURCE: CNSSI-4009

Application Developer - manage all aspects of the application development process for those business applications that support the administrative or operational functions of the company or the applications needed to serve customers effectively. SOURCE: Separation of Test, Development, and Production Environments workgroup (added per ISSC July 8, 2011)

Application Tester - uses and tests software for the purpose of locating and eliminating bugs in the product. Performing specific tests, they examine all aspects of a product from an end-user's perspective. SOURCE: Separation of Test, Development, and Production Environments workgroup (added per ISSC July 8, 2011)

Archived Data - Information that is retained solely for backup or archival purposes in accordance with backup policies. SOURCE: SP 800-83

ASP - "Application Service Provider". SOURCE: SP 800-83

Asset - Any item that is purchased by, owned by, leased to, contracted by, operated by, used by, controlled by, given to, supplied by, or in any other matter connected to Metropolitan Government. This includes everything from information on paper to enterprise computing systems, databases and networks. SOURCE: Acceptable Use Policy Work Group

Attack – Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. SOURCE: CNSSI-4009

Audit – Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. SOURCE: CNSSI-4009

Audit Log – A chronological record of system activities. Includes records of system accesses and operations performed in a given period. SOURCE: CNSSI-4009

Audit Trail – A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result. SOURCE: CNSSI-4009

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: SP 800-53; SP 800-27; FIPS 200

Authentication Credentials - Information that is used to verify the identity of a user, process or device and is a prerequisite to allowing access to other information. Includes but not limited to: passwords, SecurID PINs, and encryption keys (excluding public certificates). SOURCE: SP 800-83; SP 800-27; FIPS 200

Authenticator – The means used to confirm the identity of a user, process, or device (e.g., user password or token). SOURCE: SP 800-53; CNSSI-4009

Authorization – Access privileges granted to a user, program, or process or the act of granting those privileges. SOURCE: CNSSI-4009

Authorization Boundary – All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. SOURCE: CNSSI-4009; SP 800-53

Authorized Personnel – A person who is fully cleared and trained for access to secure areas, facilities, or information; has a valid need or job responsibility; and has been approved for access to the Physical Security Manager. SOURCE: Secured Areas Policy Work Group

Availability – Ensuring timely and reliable access to and use of information. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542

Awareness (Information Security) – Activities which seek to focus an individual's attention on an (information security) issue or set of issues. SOURCE: SP 800-50

Back Door – Typically unauthorized hidden software or hardware mechanism used to circumvent security controls. SOURCE: CNSSI-4009

Backup – A copy of files and programs made to facilitate recovery, if necessary. SOURCE: SP 800-34; CNSSI-4009

Banner – Display on an information system that sets parameters for system or data use. SOURCE: CNSSI-4009

Baseline – Hardware, software, databases, and relevant documentation for an information system at a given point in time. SOURCE: CNSSI-4009

Board – A board of Metropolitan Government.

Boundary – Physical or logical perimeter of a system. SOURCE: CNSSI-4009

Boundary Protection – Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels). SOURCE: CNSSI-4009

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. SOURCE: SP 800-28; CNSSI-4009

Business Associate Agreement (BAA) - A Business Associate Agreement is a written contract or other document between a Covered Entity and an individual or corporate "person" that: performs on behalf of the covered entity any function or activity involving the use or disclosure of Protected Health Information (PHI); and is not a member of the covered entity's workforce. A BAA ***does not*** apply to disclosures by a covered entity to a health care provider for treatment purposes disclosures to the plan

sponsor by a group health plan, or a health insurance issuer or HMO with respect to a group health plan, nor to the collection and sharing of PHI by a health plan that is a public benefits program and an agency other than the agency administering the health plan, in order to determine eligibility or enrollment.

The Business Associate Agreement (BAA) must detail permitted activities and disclosures for all Protected Health Information (PHI), and must also provide that the business associate will: not use or further disclose the PHI other than as permitted by the contract or as required by law; use appropriate safeguards to prevent unauthorized use or disclosure of the PHI, report to the covered entity any unauthorized use or disclosure of which it becomes aware; ensure that any agents, including subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to the business associate and ; on termination of the contract, return or destroy all PHI in its possession, or where that is not possible, extend the protections of the contract for as long as the information is retained.

Business Continuity Plan (BCP) – The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. SOURCE: SP 800-34; CNSSI-4009

Cardholder Data - Data as defined by the Payment Card Industry (PCI) Security Standard Council, which is the full magnetic stripe, or the Primary Account Number (PAN) plus any of the following:

- Cardholder name,
- Expiration date, or
- Service Code (Capitalized terms in this definition have the meanings set forth in the PCI Data Security Standard)

Certify General Compatibility - A commercially reasonable process or means to test that a IT Product will still operate without diminishing its functionality or speed of processing data and all functions are still available and functioning properly after some change to the IT Product or to its dependent third party product, such as after a Security Patch has taken place. SOURCE: SP 800-83

Chair – A chair of a Metropolitan Government board.

Chief Information Security Officer (CISO) – The CISO who reports to the Director of Information Technology Services.

Code – System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. SOURCE: CNSSI-4009

Confidentiality – Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: Executive Order No. 038; Confidentiality Agreements Work Group

Configuration Control – Process of controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications prior to, during, and after system implementation. SOURCE: SP 800-53 Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation. SOURCE: CNSSI-4009

Configuration Control Board – (CCB) A group of qualified people with responsibility for the process of

regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system. SOURCE: CNSSI-4009

Contingency Plan – Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions. SOURCE: CNSSI-4009

Continuous Monitoring – The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) the development of a strategy to regularly evaluate selected IA (information assurance) controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information-sharing decisions involving the enterprise. SOURCE: CNSSI-4009

Contractor Agent – Any subcontractor, independent contractor, officer, director, employee, consultant or other representative of Contractor, whether under oral or written agreement, whether an individual or entity. SOURCE: Metro Government Legal Department

Contractor Managed System - Any system, device or application which is owned, leased or rented by Metro Government or its Affiliates, which is managed or administered by Contractor on behalf of Metro Government or its Affiliates, and, any Contractor-owned systems which reside on the Metro Government IT Network and managed or administered by Contractor. SOURCE: Metro Government Legal Department

Cookie – A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. SOURCE: SP 800-28

Countermeasure – Actions, devices, procedures, or techniques that meet or oppose (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. SOURCE: CNSSI-4009

Critical Security Patch - Security Patch that mitigates or remedies a Critical Vulnerability.

Critical Vulnerability - Vulnerability that would allow an individual or system without access rights or proper credentials to gain administrative-like access to a IT Product or Service or to data contained therein or whose exploitation could allow code execution without user interaction.. For example, a compromise that would allow authorized unfettered or administrative-like access, include without limitation, administrative access to the IT Product or Service, full access or control of a data store, and/or the ability to alter Audit Logs. Determination of “Critical” is determined by the vendor’s assessment of the vulnerability or of a Common Vulnerability Scoring System base score of “high”. SOURCE: SP 800-83

Cryptographic – Pertaining to, or concerned with, cryptography. SOURCE: CNSSI-4009

Cryptographic Controls - A set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the control. SOURCE: Policy 10.4

Cryptographic Key – A parameter used in conjunction with a cryptographic algorithm that determines (1) the transformation of plaintext data into ciphertext data; (2) the transformation of ciphertext data into plaintext data; (3) a digital signature computed from data, (4) the verification of a digital signature computed from data; (5) an authentication code computed from data; or (6) an exchange agreement of a shared secret. SOURCE: FIPS 140-2

Cryptographic Module – The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. SOURCE: FIPS 140-2

Cryptography – 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

Data – A subset of information in an electronic format that allows it to be retrieved or transmitted. SOURCE: CNSSI-4009

Data Breach - Any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Data Information, or actual or suspected loss of Metro Government Data Information.

Data Custodian - Responsible for providing a secure infrastructure in support of the data, including, but not limited to, backup and recovery processes, granting access privileges to system users as authorized by Data Owners, and implementing and administering controls over the information. SOURCE: Separation of Test, Development, and Production Environments workgroup (added per ISSC July 8, 2011)

Defense-in-Depth – Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. SOURCE: CNSSI-4009; SP 800-53

Denial of Service (DoS) – An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. SOURCE: SP 800-61 The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) SOURCE: CNSSI-4009

Department – A department of Metropolitan Government.

Department Heads – The director or chairperson of any Metropolitan Government department agency or board to which this policy applies, including the Mayor. SOURCE: Separation of Development, Test, and Operational Facilities Work Group

Director – A director of an agency or department of Metropolitan Government.

Disaster Recovery Plan (DRP) – A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. SOURCE: SP 800-34

Discretionary Access Control – A means of restricting 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: CNSSI-4009

Distribution Date – The date of policy release to department heads. SOURCE: ISSC

Domain – A set of subjects, their information objects, and a common security policy. SOURCE: SP 800-27 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. See also security domain. SOURCE: CNSSI-4009; SP 800-53

Education (Information Security) – Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge and strives to produce IT security specialists and professionals capable of vision and proactive response. SOURCE: SP 800-50

Effective Date – The date employees and departments are responsible for full policy compliance and accountable for deviations. SOURCE: ISSC

Electromagnetic Signals Emanation – Unintentional signal or noise appearing external from equipment that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any information processing equipment. SOURCE: Secured Areas Policy Work Group

Electronic Protected Health Information - "EPHI" means PHI as defined in 45 C.F.R. 160.103 of the HIPAA regulations in electronic form. SOURCE: Metro Government Legal Department

Electronic Signature – The process of applying any mark in electronic form with the intent to sign a data object. See also digital signature. SOURCE: CNSSI-4009

Email - Any means of electronic communication transmitted under Simple Mail Transfer Protocol (SMTP), or a similar protocol, in which (a) usually text and/or attachments are transmitted, (b) operations include sending, storing, processing, and receiving information, (c) Users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee. SOURCE: Acceptable Use Policy Work Group

Emanations Security (EMSEC) – Protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emissions from crypto-equipment or an information system. See TEMPEST. SOURCE: CNSSI-4009

Encryption – Conversion of plaintext to ciphertext through the use of a cryptographic algorithm. SOURCE: FIPS 185

Enterprise Architecture (EA) – The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture. SOURCE: CNSSI-4009

Exception - Any approved action that does not normally comply with Metropolitan Government policies, standards and practices. SOURCE: Acceptable Use Policy Work Group

Executive Order – An Executive Order of the Mayor of Metropolitan Government.

External Devices - Any non-Metropolitan Government issued and third-party privately-owned desktop and Mobile Devices involved in remote access to Metropolitan Government's non-public computing resources. SOURCE: Acceptable Use Policy Work Group

External Information System (or Component) – An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. SOURCE: SP 800-53; SP 800-53A; CNSSI-4009

External Information System Service – An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. SOURCE: SP 800-53; CNSSI-4009

External Information System Service Provider – A provider of external information system services to an organization through a variety of consumer-producer relationships, including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. SOURCE: SP 800-53; SP 800-53A; Confidentiality Agreements Work Group

Facility Access Authority – responsible for approving physical access requests for a particular secured facility, building, room, or area. SOURCE: Secure Areas workgroup (added per ISSC July 8, 2011)

Facility Manager – responsible for implementing and maintaining facility utilities and physical maintenance (i.e. HVAC, electric, emergency power, fire protection, water, etc.). SOURCE: Secure Areas workgroup (added per ISSC July 8, 2011)

Facility Security Manager – responsible for ensuring that all applicable physical controls are implemented and maintained, and that procedures related to day-to-day administrative and operational management are documented and reviewed in accordance with all applicable laws, regulations, policies and procedures. SOURCE: Secure Areas workgroup (added per ISSC July 8, 2011)

Firewall – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. SOURCE: CNSSI-4009

Firmware – The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution. SOURCE: FIPS 140-2

Flaw – Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. SOURCE: CNSSI-4009

Forensics – The practice of gathering, retaining, and analyzing computer-related data for investigative

purposes in a manner that maintains the integrity of the data. SOURCE: SP 800-61; CNSSI-4009

Hardware – The physical components of an information system. See software and firmware. SOURCE: CNSSI-4009

Head – A head of a Metropolitan Government department or agency.

HIPAA - Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations related thereto. SOURCE: Metro Government Legal Department

Honeypot - A mechanism set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems, generally consisting of a computer, data, or a network site that appears to be part of a network, but is actually isolated, unprotected, and monitored, and which seems to contain information or a resource of value to attackers. SOURCE: Policy 10.4

IAAS - "Infrastructure As A Service." SOURCE: SP 800-83

Identification – The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. SOURCE: SP 800-47

Identifier – Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. SOURCE: FIPS 201

Identity – The set of physical and behavioral characteristics by which an individual is uniquely recognizable. SOURCE: FIPS 201

Inappropriate Usage – A person violating acceptable computing use policies. SOURCE: SP 800-61

Important Security Patch - A Security Patch that mitigates or remedies an Important Vulnerability.

Important Vulnerability - A Vulnerability in the IT Product or Service that would allow a user who already had access to the IT Product or Service to obtain unauthorized access rights or compromise the IT Product or Service in some way or whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. Determination of "Important" is determined by the vendor's assessment of the vulnerability or of a Common Vulnerability Scoring System base score of "medium". SOURCE: SP 800-83

Incident Handling – The mitigation of violations of security policies and recommended practices. SOURCE: SP 800-61

Information – An instance of an information type. SOURCE: FIPS 200; FIPS 199; SP 800-60; SP 800-53 Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. SOURCE: CNSSI-4009

Information Flow Control – Procedure to ensure that information transfers within an information system are not made in violation of the security policy. SOURCE: CNSSI-4009

Information Owner – Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing,

dissemination, and disposal. SOURCE: CNSSI-4009

Information Security – Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Confidentiality - Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- Integrity - Guarding against improper information modification or destruction, and protecting information nonrepudiation and authenticity; and
- Availability - Ensuring timely and reliable access to and use of information. SOURCE: Executive Order No. 038

Information Security Breach - Incident where acquisition of computerized data by an unauthorized person materially compromises the security, confidentiality, or integrity of the information. SOURCE: TCA Section 47-18-2107

Information Security Event – Any observable occurrence in a system or network that has a negative consequence SOURCE: NIST SP 800-61.

Information Security Incident – An occurrence that actually 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: FIPS 200; SP 800-53; SP 800-53A

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. SOURCE: FIPS 200; FIPS 199; SP 800-53A; SP 800-60; SP 800-18; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III

Information Technology Assets - Any and all electronic devices, communication and information systems and similar technology (as listed below), owned, leased or licensed by Metropolitan Government and provided to Users for their use in connection with, or concerning, business of the Metropolitan Government, including, without limitation:

- Computer hardware, Devices, network equipment, telephones, printers, copiers, and fax machines, calculators, Removable Media, etc.
- Software, intellectual property, operating systems, firmware, source code, applications, middleware, etc.
- Procedural Information, configuration, or documentation of any of the above

SOURCE: Acceptable Use Policy Work Group

Infrastructure - Any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government IT Network. Metro Government IT Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government IT Network as part of a Service.

Integrity – Guarding against improper information modification or destruction, and protecting [against] non-repudiation and authenticity. SOURCE: Executive Order No. 038SP 800-53

Intellectual Property – Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. SOURCE: SP 800-32

Interactive User Login - The process by which a person, as opposed to a system or application, manually identifies and authenticates himself as a user of a system or device (for example, by typing in a username and password). SOURCE: SP 800-83

Interconnection Security Agreement (ISA) – A document that regulates security-relevant aspects of an intended connection between a department, agency or board and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal memorandum of understanding/agreement that defines high-level roles and responsibilities in management of a cross-domain connection. SOURCE: CNSSI-4009

Interface – Common boundary between independent systems or modules where interactions take place. SOURCE: CNSSI-4009

Internet – The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). SOURCE: CNSSI-4009

Intrusion – Unauthorized act of bypassing the security mechanisms of a system. SOURCE: CNSSI-4009

Intrusion Detection Systems (IDS) – Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.) SOURCE: CNSSI-4009

Intrusion Prevention System - A network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. SOURCE: Policy 10.4

Key – A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. SOURCE: SP 800-63

Key Management – The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. SOURCE: FIPS 140-2; CNSSI-4009

Layered Protection – See Defense in Depth. SOURCE: Security in Development and Support Processes Work Group

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

Malicious Code and Software - A program that is written intentionally to carry out annoying or harmful actions, which includes Trojan horses, viruses, and worms. SOURCE: Policy 10.4

Malware – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of

otherwise annoying or disrupting the victim. SOURCE: SP 800-83; SP 800-41 See malicious code. See also malicious applets and malicious logic. SOURCE: SP 800-53; SP 800-53A; CNSSI-4009

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: FIPS 200; SP 800-53; CNSSI-4009

Media Sanitization – The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. SOURCE: CNSSI-4009

Metropolitan Government – The Metropolitan Government of Nashville and Davidson County.

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: SP 800-53; SP 800-53A; SP 800-18

Mobile Computing - The use of portable computing devices, including, but not limited to, notebook/laptop computers, smart phones and PDAs, in conjunction with mobile communications technologies to enable Users to access the Internet and data on their home or work computers from anywhere in the world. SOURCE: Acceptable Use Policy Work Group

Mobile Devices - Portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, PDAs, cellular telephones, digital cameras, smart phones and audio recording devices). SOURCE: Acceptable Use Policy Work Group, Policy 10.4

Multifactor Authentication – Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator. SOURCE: SP 800-53

Need-To-Know – A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. SOURCE: CNSSI-4009

Network – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. SOURCE: SP 800-53; CNSSI-4009

Network Access – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). SOURCE: SP 800-53; CNSSI-4009

NIST - National Institute of Standards and Technology. SOURCE: SP 800-83

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: SP 800-53; SP 800-53A; SP 800-60; SP 800-18

Off-the-Shelf Software or "OTS" – An item that is (1) sold, leased, or licensed to the general public; (2) offered by a Contractor trying to profit from it; (3) supported and developed by the Contractor who retains the underlying intellectual property rights; (4) available in multiple, identical copies; and (5) used without modification of the internal code.

Open IT Network - Any open, unsecured or untrusted network such as the Internet. SOURCE: SP 800-83

Open Source Software - Software that is licensed pursuant to the provisions of any "open source" license agreement including, without limitation, any version of any software licensed pursuant to any GNU General Public License (GNU GPL) or GNU Lesser/Library Public License (LGPL), or Mozilla Public License (MPL), or any other license agreement that requires source code be distributed or made available in connection with the distribution of the licensed software in object code form or that limits the amount of fees that may be charged in connection with sublicensing or distributing such licensed software**. SOURCE: SP 800-83**

Organization – An entity of any size, complexity, or positioning within an organizational structure. SOURCE: SP 800-53

Packet Sniffer – Software that observes and records network traffic. SOURCE: SP 800-61; CNSSI-4009

Password – A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data. SOURCE: CNSSI-4009

Patch Management – The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. SOURCE: CNSSI-4009

Peer-to-Peer File Sharing Software -

- Means a program, application, or software that is commercially marketed or distributed to the public and that enables a file or files on the computer on which such program is installed to be designated as available for searching and copying to one or more other computers;
    - the searching of files on the computer on which such program is installed and the copying of any such file to another computer;
    - at the initiative of such other computer and without requiring any action by an owner or authorized user of the computer on which such program is installed; and
    - without requiring an owner or authorized user of the computer on which such program is installed to have selected or designated another computer as the recipient of any such file; and
    - an owner or authorized user of the computer on which such program is installed to search files on one or more other computers using the same or a compatible program, application, or software, and copy such files to such owner or user's computer; and
- Does not include a program, application, or software designed primarily:
    - to operate as a server that is accessible over the Internet using the Internet Domain Name system;

- to transmit or receive email messages, instant messaging, real-time audio or video communications, or real-time voice communications; or
- to provide network or computer security (including the detection or prevention of fraudulent activities), network management, maintenance, diagnostics, or technical support or repair. SOURCE: Acceptable Use Policy Work Group

Penetration Testing – Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. SOURCE: SP 800-115

Personally Identifiable Information (PII) - Any information that can be used to uniquely identify, contact or locate a single person, or can be used with other sources to uniquely identify a single individual, as well as any information which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. SOURCE: Acceptable Use Policy Work Group

Physical Security – The application of physical barriers and control procedures as preventative measures or countermeasures against threats to resources and sensitive information. SOURCE: Secured Areas Policy Work Group

Physical Security Manager – The person or persons who approves physical access requests for a particular secured facility, building, room, or area. SOURCE: Secured Areas Policy Work Group

Policy – The Metropolitan Government Information Security Management Policy. SOURCE: Executive Order 38

Port – A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire). SOURCE: FIPS 140-2

Principle of Least Privilege - The principle that 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: SP 800-83

Privilege – A right granted to an individual, a program, or a process. SOURCE: CNSSI-4009

Privileged User – A user that is authorized (and, therefore, trusted) to perform security- relevant functions that ordinary users are not authorized to perform. SOURCE: SP 800-53; SP 800-53A; CNSSI-4009; Confidential Agreements Work Group

Product - Any software, hardware, system, computer equipment or product provided by Contractor to Metro Government. SOURCE: Metro Government Legal Department

Product and Service Inventory - A complete, accurate and current inventory of all IT Products and Services provided by Contractor to Metro Government. SOURCE: Metro Government Legal Department

Protected Health Information or "PHI" - Shall have the meaning set forth at 45 C.F.R. 160.103 of the HIPAA regulations.

Procedures – The steps that need to be performed to meet standards and comply with the Metropolitan Government Information Security Management Policy. There are typically many procedures in place to maintain compliance. SOURCE: Executive Order No. 038

Program – The Metropolitan Government Information Security Management Program. SOURCE: Executive Order No. 038

Protocol – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information. SOURCE: CNSSI-4009

Proxy – An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. Note: This effectively closes the straight path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for e-mail. SOURCE: CNSSI-4009

Purchasing Agreement - Any agreement between Contractor and any Metro Government for the purchase, lease, licensing, acquisition, or servicing of an IT Product or provision of Services, regardless whether Metro Government has any payment obligations under the agreement. SOURCE: Metro Government Legal Department

Remediation – The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. SOURCE: SP 800-40 The act of mitigating a vulnerability or a threat. SOURCE: CNSSI-4009

Remote Access – Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet). SOURCE: SP 800-53; SP 800-18; SP 800-53A

Remote Access Software - Any technology that can provide Remote Access to the Metro Government IT Network. SOURCE: SP 800-83

Remote Control Software - Any program or application which uses Remote Access to connect to a machine, system or application and control, manage or administer such machine, system or application.

Responsible Vulnerability Disclosure - Disclosure of a Vulnerability to the Contractor by a third party where the Vulnerability is kept secret for an agreed upon time so that Contractor can create, test, document and release a Security Patch to address the Vulnerability. SOURCE: SP 800-83

Removable Media - Storage media which is designed to be removed from the computer without powering the computer off. This includes, but is not limited to, DVDs, CDs, memory cards, floppy disks, zip disks, tapes, USB flash drives, external hard disk drives. SOURCE: Acceptable Use Policy Work Group

Risk – The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: FIPS 200

Risk Assessment – The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. SOURCE: SP 800-53

Risk Management – The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; and 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system. SOURCE: FIPS 200

Risk Mitigation – Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. SOURCE: SP 800-30 Prioritizing, evaluating, and implementing the appropriate risk- reducing controls/countermeasures recommended from the risk management process. SOURCE: CNSSI-4009

Risk Reduction – Actions taken to lessen the probability, negative consequences, or both, associated with a risk. SOURCE: ISO/IEC 27002

Risk Retention – Acceptance of the burden of loss or benefit of gain from a particular risk. NOTE In the context of this International Standard, the term “activity” is used instead of the term “process” for risk estimation. SOURCE: ISO/IEC 27002

Risk Tolerance – The level of risk an entity is willing to assume in order to achieve a potential desired result. SOURCE: SP 800-32 The defined impacts to an enterprise’s information systems that an entity is willing to accept. SOURCE: CNSSI-4009

Risk Transfer – Sharing with another party the burden of loss or benefit of gain from a particular risk. NOTE In the context of information security risks, only negative consequences (losses) are considered for a risk transfer. SOURCE: ISO/IEC 27002

Risk Treatment - Process of selection and implementation of measures to modify risk. SOURCE: ISO/IEC 27002

Role – A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks. SOURCE: CNSSI-4009

SaaS - “Software as a service” or “software on demand”. SOURCE: SP 800-83

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: SP 800-53; SP 800-53A; SP 800-18; FIPS 200; CNSSI- 4009

Sanitization (Sanitize) – Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. SOURCE: FIPS 200

Secure Area – A facility, or an area, room, or group of rooms within a facility with both the physical and personnel security controls sufficient to protect information systems, equipment, and/or information. SOURCE: Adapted from the Criminal Justice Information Services Security Policy

Security – A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. SOURCE: CNSSI-4009

Security Assessment – The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. SOURCE: SP 800-53A

Security Attribute – An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy. SOURCE: SP 800-53; CNSSI-4009

Security Engineering – An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development life cycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem. SOURCE: CNSSI-4009

Security Functions – The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. SOURCE: SP 800-53

Security Impact Analysis – The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system. SOURCE: SP 800-53; SP 800-53A; SP 800-37; SP 800-18; CNSSI- 4009

Security Officer – Uniformed personnel, proprietary or contracted, whose primary responsibility is to maintain a watch of secured areas, facilities, and immediate grounds to protect against unauthorized access, fire, vandalism, property damage, and other hazards. Other duties may include: entry control, motorized or foot walking patrols, security escort of personnel or assets, inspections, and special assignments. SOURCE: Secured Areas Policy Work Group

Security Patch - A patch, bug fix, software update, upgrade, new release, new version, modification, improvement, enhancement or fix designed to repair known problems in previous software releases in

order to prevent unauthorized access, destruction, or corruption of data, or exploitation of a Vulnerability. SOURCE: SP 800-83

Security Plan – Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. SOURCE: SP 800-53

Sensitive Data - Any data classified as "Confidential" or "Restrictive" as defined by the Metropolitan Government Information Classification policy. SOURCE: Acceptable Use Work Group; Confidentiality Agreements Work Group

Sensitive Information – Any information classified as "Confidential" or "Restrictive" as defined by the Metropolitan Government Information Classification Policy. SOURCE: Acceptable Use Policy Work Group; Confidentiality Agreements Work Group

Sensitivity – A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. SOURCE: SP 800-60; CNSSI-4009; Confidentiality Agreements Work Group

Service-Level Agreement – Defines the specific responsibilities of the service provider and sets the customer expectations. SOURCE: CNSSI-4009

Service(s) - Any service provided by Contractor (or its Contractor Agents) to Metro Government, including but not limited to, maintenance and support service, program development service, consulting service, outsourcing service, or other professional service. SOURCE: CNSSI-4009

Session Timeout - A a security control or function that automatically logs a user off and ends the current use session of the IT Product after a defined period of inactivity. SOURCE: SP 800-83

Social Engineering – A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. SOURCE: SP 800-114

Software – Computer programs and associated data that may be dynamically written or modified during execution. SOURCE: CNSSI-4009

Software Development Life Cycle – See System Development Life Cycle. SOURCE: Security in Development and Support Processes Policy Work Group

Software Owner – See System Owner. SOURCE: Security in Development and Support Processes Policy Work Group

Split Tunneling - A technology that allows a VPN User to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. SOURCE: Acceptable Use Policy Work Group

Spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system. 2. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating masquerading, piggybacking, and mimicking are forms of spoofing. SOURCE: CNSSI 4009

Spyware – 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: SP 800-53; SP 800-53A; CNSSI-4009

Standards – The Metropolitan Government minimum requirements for users to assure compliance with the Metropolitan Government Information Security Management Policy. SOURCE: Executive Order No. 038; Acceptable Use Policy Work Group

Steering Committee – The Metropolitan Government Information Security Steering Committee. SOURCE: Executive Order 38

Store – Act of backing up, saving, keeping, recording or otherwise writing or storing any data or information in any type of permanent media or permanent storage device. For the avoidance of doubt, this excludes temporarily storing information to a dynamic and volatile RAM.

Streaming Media - Any multimedia that is constantly received by and presented to an end-User. SOURCE: Acceptable Use Policy Work Group

Strong Authentication - An authentication system that leverages two different types of data that serve as proof of the identity of the specific user trying to authenticate (e.g., a certificate and a password, a password and the answer to a secret user question, SecurID Token Code and PIN, or a password and encrypted session cookie). User Identifiers (UIDs) are never considered one of the factors in Strong Authentication. SOURCE: SP 800-83

Strong Encryption – An Encryption algorithm that meets industry standard criteria, as defined by NIST. Whenever External Parties are required to use Strong Encryption the cryptographic modules used must be validated to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. SOURCE: SP 800-83

Strong Hash Algorithm - A hash value that is commercially resistant to forgery. The strength of the hash algorithm is an industry standard as defined by NIST. SOURCE: SP 800-83

Supply Chain – A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. SOURCE: SP 800-53; CNSSI-4009

Supply Chain Attack – Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. SOURCE: CNSSI-4009

System – SEE Information System. SOURCE: SP 800-53

System Administrator – A person who manages the technical aspects of a system. SOURCE: SP 800-40 (added per ISSC July 8, 2011). Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures. SOURCE: CNSSI-4009

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: SP 800-34; CNSSI-4009

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

Technical Controls – The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. SOURCE: SP 800-53; SP 800-53A; SP 800-18; FIPS 200

Telecommunications – Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means. SOURCE: CNSSI-4009

Telework - Ability for Metropolitan Government's employees and contractors to perform work from locations other than Metropolitan Government's facilities. Teleworkers use various client devices, such as desktop and laptop computers, cell phones, and personal digital assistants (PDA), to read and send E-mail, access Web sites, review and edit documents, and perform many other tasks. Most Teleworkers use remote access, which is the ability for Metropolitan Government's Users to access its non-public computing resources from external locations other than Metropolitan Government's facilities. SOURCE: Acceptable Use Policy Work Group

Teleworker - Means a user who teleworks. SOURCE: Acceptable Use Policy Work Group

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800- 61; SP 800-18; CNSSI-4009

Threat - A potential cause of an unwanted incident, which may result in harm to a system or organization. SOURCE: ISO/IEC 27002

Training (Information Security) – Training strives to produce relevant and needed (information) security skills and competencies. SOURCE: SP 800-50

Transmission – The state that exists when information is being electronically sent from one location to one or more other locations. SOURCE: CNSSI-4009

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

Trustworthiness – The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned

responsibilities. SOURCE: SP 800-79 The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. SOURCE: CNSSI-4009 Security decisions with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities. SOURCE: FIPS 201

Unauthorized Access – Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use. SOURCE: FIPS 191

User - All Metropolitan Government employees, independent contractors, consultants, temporary or part-time employees, leased employees, interns, and other persons or entities to whom Metropolitan Government has explicitly granted access to Metropolitan Government's Information Technology Assets and Information. SOURCE: Acceptable Use of Information Technology Assets Policy Work Group; Confidential Agreements Work Group

Virtual Private Network (VPN) – Protected information system link utilizing tunneling, security controls (see Information Assurance), and endpoint address translation giving the impression of a dedicated line. SOURCE: CNSSI-4009

Virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. SOURCE: CNSSI-4009

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: SP 800-53; SP 800-53A; SP 800-18; SP 800-60; SP 800- 61; SP 800-115; FIPS 200

Vulnerability Analysis – SEE Vulnerability Assessment.

Vulnerability Assessment – Formal description and evaluation of the vulnerabilities in an information system. SOURCE: SP 800-53; SP 800-53A; SP 800-18; CNSSI-4009

Wireless Access Point (WAP) – A device that acts as a conduit to connect wireless communication devices together to allow them to communicate and create a wireless network. SOURCE: CNSSI-4009

Wireless Technology – Technology that permits the transfer of information between separated points without physical connection. Note: Currently wireless technologies use infrared, acoustic, radio frequency, and optical. SOURCE: CNSSI-4009

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See malicious code. SOURCE: SP 800-61; CNSSI-4009

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300

SIGNATURE

_____
Keith Durbin,
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

44 U.S.C Section 3502
44 U.S.C Section 3542
CNSSI 4009, *National Information Assurance (IA) Glossary*
FIPS 140-2, *Security Requirements for Cryptographic Modules*
FIPS 185, *Escrowed Encryption Standard*
FIPS 191, *Guideline for the Analysis of Local Area Network Security*
FIPS 199, *Standards for Security Characterization of Federal Information and Information Systems*
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*
Karl Dean Executive Order No. 38
OMB Circular No. A-130 Appendix III
NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*
NIST Special Publication 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*
NIST Special Publication 800-27 Rev A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
NIST Special Publication 800-28 Version 2, *Guidelines on Active Content and Mobile Code*
NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
NIST Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*
NIST Special Publication 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems (Errata Page – Nov 11, 2010)*
NIST Special Publication 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST Special Publication 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program*
NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*
NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
NIST Special Publication 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST Special Publication 800-53A Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems*
NIST Special Publication 800-60 Rev 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
NIST Special Publication 800-61 Rev 1, *Computer Security Incident Handling Guide*
NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication Guideline*
NIST Special Publication 800-66 Rev 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification(PIV) Card Issuers (PCIs)*

NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*
NIST Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*
NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*
Metropolitan Information Security Management Program Work Group *Acceptable Use of Information Technology Assets*
Metropolitan Information Security Management Program Work Group *Confidentiality Agreements*
Metropolitan Information Security Management Program Work Group *Secured Areas*
Metropolitan Information Security Management Program Work Group *Security in Development and Support Processes*
Metropolitan Information Security Management Program Work Group *Separation of Development, Test, and Operational Facilities*

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.0	10/8/2010	First released version
1.1	7/19/2011	Added definitions recommended by ISSC July 8, 2011
1.2	11/30/2015	Added definitions from the Information Security Agreement
1.3	7/30/2017	Added definitions for "breach" and "event"