Department of Information Technology
State of North Carolina

Statewide Glossary of Information Technology Terms

July 2018

Table of Contents

PURPOSE 3

SCOPE 3

GLOSSARY OF TERMS 3

General 3
A 3
B 10
C 14
D 25
E 32
F 36
G 40
H 41
I 43
J 50
K 50
L 50
M 52
N 56
O 58
P 61
Q 70
R 71
S 75
T 84
U 87
V 88
W 91
X 93
Y 93
Z 93

PURPOSE

The purpose of this Glossary of Terms is to provide a central repository of terms that apply to documentation created and maintained by the North Carolina Office of the State Chief Information Officer (State CIO).

SCOPE

This document covers all State information technology areas that fall under the responsibility of the State CIO. The definitions apply to statewide information technology policies, standards and the statewide architecture for all government agencies of the State of North Carolina.

HISTORY

This glossary was first published in 2005. It has been updated as terms were added or changed to the information technology and security lexicon. This edition of the Glossary was updated and published in July 2018.

GLOSSARY OF TERMS

GENERAL

3- Way Handshake – Machine A sends a packet with a SYN flag set to Machine B. B acknowledges A's SYN with a SYN/ACK. A acknowledges B's SYN/ACK with an ACK.

A

ACL – Access Control List

ACWP – Actual Cost of Work Perform

AES – Advanced Encryption Standard

AP – Access point

APT – Advanced Persistent Threat

ARP – Address Resolution Protocol

Abstraction – A representation of an entity that contains less information than the entity.

Acceptance – Final approval and receipt of a product or service by the customer.

Acceptance Criteria – The list of requirements that must be satisfied prior to the customer accepting delivery of the product.

Acceptance Management – The process used throughout the project to obtain approval for products or services.

Acceptance Test – Formal user testing performed prior to accepting the system (sometimes called client acceptance test or user acceptance test).

Access – Instruct, communicate with, cause input, cause output, cause data processing or otherwise make use of any resources of a computer, information system or information network.

Access Control – A feature or technique used to permit or deny use of the components of a system, including hardware, software and/or procedures that restrict access to devices and services.

Access Control List (ACL) – A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Point (AP) – A device that connects to a wired network and sends and receives radio signals enabling wireless access to a telecommunication network by wireless devices.

Accessibility – Access to information for people with disabilities comparable to that accorded people without disabilities.

Accountability – The property that enables activities on a system to be traced to an individual.

Accuracy – A quantitative measure of the magnitude of error, preferably expressed as a function of the relative error, a high value of this measure corresponding to a small error.

Acquisition – Generic term for hardware, software, or services acquired from an outside vendor or contractor.

Action Plan – A plan that describes what needs to be done and when it needs to be completed. Project plans are action plans.

Activation – The implementation of a Continuity plan, whether in whole or in part. (FEMA)

Activity – An element of work performed in a project. An activity has precise starting and ending dates, incorporates a set of tasks to be completed, consumes resources, and produces tangible results. Activities are often subdivided into tasks and multiple activities may compose a phase. (PMI)

Activity Definition – Identification of the specific activities that must be performed to produce project deliverables. (PMI)

Activity Description – Short phrase or label used in a network diagram to describe the scope of work for the activity. (PMI)

Activity Duration Estimate – Estimation of the amount of work that will be needed to complete an activity.

Actual Cost of Work Performed (ACWP) – Total costs incurred (direct and indirect) in accomplishing work during a given time period.

Actual Finish Date – A point in time when work actually ended for the task or activity.

Actual Start Date – The point in time that work actually began on the task or activity.

Adaptive Maintenance – Software maintenance performed to make a computer program usable in a changed environment. (IEEE)

Adaptive System – Describes software that has flexibility as the primary design point that enables the system to adapt quickly and easily to changes in technology and in interfacing with other systems. An adaptive system can be explained through a comparison of jigsaw puzzles to LEGOs: both are small "plug in" components. But a puzzle goes together in only one way and a puzzle piece from one puzzle does not fit into another puzzle. LEGO pieces can be used to build different things and are easy to change, as business needs change.

Address Resolution Protocol (ARP) – Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Adherence – The process or activity in following a set of specific rules.

Administration – The functions required to establish, manage, and maintain security.

Administrative Access – Access to servers or other devices with the intent to perform administrative functions.

Advanced Encryption Standard (AES) – An encryption algorithm for securing sensitive but unclassified material by U.S. government agencies.

Advanced Persistent Threat (APT) – A network attack in which an unauthorized person gains access to a network and remains undetected for a long period of time in order to steal data, rather than cause damage to the organization. The characteristics of APT are as follows:

- Purposeful with defined objectives
- Resourceful

- Sophisticated methods and technology
- Substantially funded for ongoing efforts

Adware – Adware is included as part of a software program that is offered at a free or reduced fee in exchange for viewing advertisement banners or pop-ups. Often times, adware includes a code component that tracks user activity and other information and passes it to third parties without the user's knowledge or direct consent. This practice is also known as "spyware." Careful attention to license agreements will often expose these practices. Agency policy and legal counsel can determine if use of this type of software is appropriate.

Agency – Any department, institution, commission, committee, board, division, bureau, office, officer, or official of the State of North Carolina that is subject to the State CIO's policies and standards. The term does not include a State entity excluded from coverage under G.S. § 143B-1300, unless that State entity elects to be covered.

Agency Network – A network used by a State of North Carolina governmental entity that is considered internal to the agency and separate from other networks. An agency network may be considered a private network if it is segregated from a public network (i.e., the State's Network or the Internet) by firewalls with appropriate rulesets. If an agency network is not appropriately segregated from other public networks, the agency network is considered to be a public network.

Agency Technical Architecture – The Agency Technical Architecture provides direction on specific technology choices and specifies vendor preference, including hardware and software choices, as opposed to the Statewide Architecture Framework, which is high level and vendor neutral.

Agreement – A project agreement is a document, or set of documents, that defines the scope, duration, cost, and deliverables for a project. A project agreement may take the form of a statement of work (SOW), project concept document (Charter), or a business contract.

Algebraic Language – A programming language that permits the construction of statements resembling algebraic expressions, such as X = Y + 5; e.g., FORTRAN. (IEEE)

Algorithm – A precise set of ordered instructions for carrying out some computation.

Algorithmic Language – A programming language designed for expressing algorithms; e.g., ALGOL. (IEEE)

All-Hazards – The spectrum of all types of hazards including accidents; technological events; natural disasters; terrorist attacks; warfare; and, chemical, biological (including pandemic influenza), radiological, nuclear, or explosive events. (FEMA)

Allocation – The process of distributing requirements, resources, or other entities among the components of a system. (IEEE)

Alphanumeric – A combination of alphabetic letters, numbers, and special characters.

Alpha Testing – A testing period in which pre-release versions of software products are given to a select group of users before the product is officially deployed.

Alternate Sites – Alternate sites are locations other than the primary facility used to carry out Essential Functions by relocating ERG members following activation of the Continuity Plan. These sites refer to facilities, locations, and also work arrangements such as telework and mobile work concepts. (FEMA)

Anomaly – Anything observed that deviates from expectations. (IEEE Standard 1012)

Applet – Java programs; an application program that uses the client's web browser to provide a user interface.

Application – A computer system (potentially including multiple programs, modules, etc.) designed to accomplish operational tasks or functions that help a user perform his or her work. Applications typically fall into one of four categories: Core Business; Desktop; Common Services & Integration; and Process Automation. It is also a generic term for a program or system that handles a specific business function.

Application Access – Access to one application from another when applications reside on different servers and must cross network zones to connect.

Application Architecture – Identifies criteria and techniques associated with the design of an application.

Application Category – Hierarchical classification of application type(s). Used to filter and group for analysis and reporting.

Application Criticality – Application criticality has the following categories.

- *Statewide Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to statewide core functions, processes and/or activities. The applications loss may also impact a large portion of the State's population.

- *Department Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to this department's core functions, processes and/or activities.

- *Program Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to the core functions, processes and/or activities associated with a program within an agency.

- *Non Critical* – From an information technology perspective, in the agency's opinion, the loss of this application will have little or no impact to statewide and/or this department's core functions, processes and activities or the core functions, processes and activities associated with a program within an agency.

Application Domain – Identifies criteria and techniques associated with the design of applications for the state's distributed computing environment that can be easily modified to respond quickly to the state's changing business needs. *See,* Statewide Architecture Framework for more information.

Application ID/Name – An identifier/label assigned to an application in order to identify it.

Application Server – Viewed as both hardware and software, an application server is a server program in a computer in a distributed network that provides the business logic for an application program. The application server is also viewed as part of a n-tier application, consisting of a graphical user interface (GUI) server, an application (business logic) server, and a database. It may also be defined as a program that handles application operations between users and an organization's backend business applications or databases.

Application Software – Software designed to fulfill specific needs of a user. (IEEE)

Application Support Activities – Changes to an application that sustain, but do not create, a business application asset (such as PeopleSoft or Passport support).

Application System – A set of computer programs, data files, and related procedures that perform a set of related functions.

Approval Cycle – Process of gaining funding and management approval prior to project initiation.

Approximation – A judgment on the order of magnitude of a systems project. The judgment is based on personal experience and knowledge of the general area. Approximations have a much lower level of accuracy than estimates based on work plans but have a higher degree of accuracy than sizings which are "ballpark" estimates.

Architecture – A framework that describes an organizational structure or set of guidelines intended to provide enterprise direction.

Architecture Framework – A single, common, and cohesive vision that directs the design, construction, purchase, deployment, and management of information systems (IS) and information technology (IT) across state government.

Architectural Principles – Those principles that guide the design of business component structures that are highly granular and loosely coupled with well-defined standards for process integration and information exposure. The principles provide guidance on what is important in

the creation, selection, and implementation of technology. Guiding statements of position that communicate fundamental elements, truths, rules, and qualities that must be exhibited by an enterprise. Architectural principles are also used as evaluation criteria in the absence of detailed standards or practices to direct technology decision-making.

Architectural Standard Practice – An established practice that supports IT projects and systems to improve the outcome, diminish risks, and increase reliability. Standard practices are recognized in the industry as replicable, transferable, and adaptable across department and division lines, and shown to produce superior results when applied. Standard practices must be applied to IT infrastructure, applications, and projects for North Carolina state agencies under the purview of the State CIO. All other agencies both State and local are encouraged to apply these practices.

Architectural Standards – Identified as industry standards (international, national, standards bodies, or de facto) that apply to technology domains and are adopted for use by the State of North Carolina. Statewide Architecture Framework standards must be applied to IT infrastructure, applications, and projects for North Carolina State agencies under the purview of the State CIO. All other agencies both State and local are encouraged to apply these standards.

Argument – An independent variable.

Assessment – A general term for the formal management review of a process. Refers to the process of collecting evidence of performance against plan. It can also be the act of determining an importance / value of an entity.

Asset Management – A series of integrated processes that monitor all aspects of IT system employment during their life cycle. IT assets are managed through the development of business metrics associated with procurement, personnel, cost, operations, performance, changes, disposal and refreshment. This enables IT to better align with the accomplishment of business goals and objectives.

Assurance – Those activities that demonstrate the conformance of a product or process to specified criteria.

Assurance Plan – A document containing the technical and planning aspects of the assurance activities for a software development or acquisition project. Sometimes called the Software Quality Assurance Plan (SQAP).

Asymmetric Key Cryptography – A method of cryptography in which different keys are used to encrypt and decrypt, as contrasted with symmetric key cryptography. Also called “public key cryptography” because one of the keys is typically made public (the other is kept private).

Attribute – A named property of an entity.

Audit – The process of reviewing system activities that enables the reconstruction and examination of events to determine if proper procedures have been followed.

Authentication – The process of determining whether someone or something is, in fact, who or what it is declared to be (verifying the identity of the user) based upon credentials provided such as a user ID and password combination. It is the act of identifying or verifying the eligibility of a workstation, originator, or individual to access specific categories of information.

Authentication and Authorization Service – Founded in directory based services and a core technology for securing the state's infrastructure. This is a service operated by DIT, known as NCID.

Authentication Header (AH) – Sender authentication and integrity, but not confidentiality. *See,* Internet Protocol Security (IPSec).

Authorization – The process of granting a user access to information, a system or an application. Often access privileges are granted based on the role the user has in relation to the organization and/or the system to be accessed.

Authorization and Access Control – The means of establishing and enforcing rights and privileges allowed to users.

Authorized User – A person, system, application or defined group that has been authenticated to an information technology (IT) system and granted access only to those resources which he or she has been permitted to use.

Automated Business System – A business line where transactions for service delivery are performed in an automated IT environment.

Availability – The need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

B

BAC – Budget at Completion

BCM – Business Continuity Management

BCP – Business Continuity Plan

BCWP – Budgeted Cost of Work Performed

BCWS – Budgeted Cost of Work Scheduled

BGP – Border Gateway Protocol

BIA – Business Impact Analysis

BIND – Berkeley Internet Name Domain

BYOD – Bring Your Own Device

Backdoor – A backdoor is a secret or undocumented means of getting into a computer system. Many programs have backdoors placed by programmers to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by kickers once they gain access to allow themselves an easier way around any security mechanisms that are in place the next time they enter or in case their original entrance is discovered.

Backup – The process of duplicating data stored on a computer's hard disk to another storage medium for the purpose of system and/or data restoration to its original state following a disaster or other inadvertent loss. Backup may also refer to alternative processing capabilities through secondary systems.

Balanced Scorecard – Performance measurement system that allows both financial and non-financial objectives to be assessed for the purpose of making strategic business decisions.

Bar Chart – A management tool, synonymous with Gantt Chart, used to plan and control the time and schedule elements of a project. The chart lists the major activities of the project, scheduled start and ending times, and current status (progress). The primary advantage of the bar chart is that the plan (schedule) and progress of the project can be portrayed graphically. Activities and other project elements are listed down the left side of the chart, dates are shown across the top, and activity durations are shown as date-placed horizontal bars.

Baseline – A specification or product that has been formally reviewed and agreed upon and that can be changed only through formal change control procedures. Baselines are usually deliverables and provide the basis for future work. (PMI)

Baseline Plan – The initial approved plan to which deviations will be compared as the project proceeds. A work product that has been formally approved and that can be changed only through formal change control procedures.

Batch – A term describing a method of operating computers. A transaction processing method that executes groups of transactions and returns the results, all without human intervention.

Benchmark – A defined measurement or standard that serves as a point of reference by which process performance is measured.

Benchmarking – The process of measuring products, services, and business practices against those of recognized industry leaders.

Benefit to Cost Ratio – Determination of the dollars returned for every dollar invested.

Berkeley Internet Name Domain (BIND) – an implementation of DNS. DNS is used for domain name to IP address resolution.

Best Practice – A proven technique or methodology established from lessons learned that support IT projects and systems to accomplish the following: increase the reliability, help improve the outcome, and diminish the risk. Best practices are recognized as replicable, transferable, adaptable, and shown to produce superior results.

Beta Testing – A process similar to alpha testing except that it occurs after alpha testing and prior to product release.

Big-Bang Approach – A type of hardware / software integration where all of the project elements are combined all at once into one overall system, rather than in stages.

Biometrics – Unique, measurable physical or behavioral characteristics of a human being for automatically recognizing or verifying identity. Biometrics use physical characteristics of the users to determine identity and access.

Black Box Testing – Testing that verifies that a given input produces the expected output without knowledge of the code.

Block Diagram – A diagram of a system represented by suitably annotated geometrical figures. (IEEE)

Block-Structured Language – A programming language in which sequences of statements (blocks) are defined with begin and end delimiters and variables are not recognized outside the block (e.g., ADA, ALGOL, PL/1). (IEEE)

Boot – To initialize a computer system by clearing memory and reloading the operating system. (IEEE)

Border Gateway Protocol (BGP) – An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

Bot – An automated software program that can execute certain commands when it receives a specific input (like a ro-"bot").

Bottom-up – Pertaining to an activity that starts with the lowest level component of a hierarchy proceeding to progressively higher levels. (IEEE)

Brainstorming – Technique used to generate creative ideas through the spontaneous interaction of a group.

Breach – An incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner. A data breach can occur with a small company or a large organization, and it may involve sensitive, proprietary, or confidential information, such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property. Also called Cyber Breach or Data Breach.

Bridge – A device that connects two separate local area networks (LANs). Once bridging is accomplished, the bridge makes interconnected networks look like a single network.

Bring Your Own Device (BYOD) – A policy of permitting employees to bring personally owned mobile devices (e.g., laptops, tablets, and smart phones) to their work, and to use those devices to access work-related information and applications.

Broadcast Address – An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

Browser-Based – A system where the presentation tier of the application is delivered using a standard Internet browser.

Budget at Completion (BAC) – The estimated total cost of the project at completion.

Budgeted Cost of Work Performed (BCWP) – The sum of the approved cost estimates for activities completed during a given period of time.

Budgeted Cost of Work Scheduled (BCWS) – The sum of the approved cost estimates for activities scheduled to be performed during a given period of time.

Bug – An error in a program or fault in a piece of equipment.

Business Case – Financial analysis of the cost versus benefit of a proposed project.

Business Associate Agreement (BAA) – A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. According to the HIPAA Privacy Rule, the types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the HIPAA Administrative Simplification Rules.

Business Continuity Management (BCM) – The advance planning and preparations which are necessary to identify the impact of potential technology losses, develop and test recovery plan(s) which ensure continuity of business services in the event of an emergency or disaster, and administer a comprehensive training, testing and maintenance program.

Business Continuity Plan(ning) (BCP) – A strategic plan that outlines the organization's goals,

objectives, and procedures for preserving the continuity of its critical information technology systems under adverse or degraded conditions. The Business Continuity Plan incorporates other plans including disaster recovery, end-user recovery, contingency, response, and crisis management plans.

Business Continuity Risk Management – An impact analysis for those risk outcomes that disrupt agency business, specifically information technology systems.

Business Function – A process or procedure undertaken by a business as a discrete operation. Examples include payroll and personnel systems, etc.

Business Impact Analysis (BIA) – A management level analysis, which identifies the impacts of losing organizational information technology resources. A BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

Business Logic – The part of an application program that performs the required data processing of the business. The routines that perform the data entry, update, query and report processing.

Business Objectives – Broadly defined statements that describe what the organization must accomplish in order to achieve its goals and expectations.

Business Process – A collection of related, structured activities or chain of events that produce a specific service or product for an internal or external customer.

Business Process Analysis (BPA) – A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, and facilities inherent in the execution of a function or requirement. (FEMA)

Business Rules – A set of practices associated with certain business processes that are required by regulation, law, accounting controls, or common practice.

C

C&C (or C2) – Command and Control

CA – Certificate Authority

CAP – Corrective Action Plan or Corrective Action Program

CASB – Cloud Access Security Broker

CASE – Computer Aided Software Engineering

CCB – Change Control Board

CCMP – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CDM – Continuous Diagnostics and Mitigation

CERT – Computer Emergency Response Team

CHAP – Challenge-Handshake Authentication Protocol

CJI – Criminal Justice Information

CMM – Capability Maturity Model

COG – Continuity of Government

COOP – Continuity of Operations

COTS – Commercial Off-the-Shelf

CPI – Cost Performance Index

CSP – Cloud Service Provider

CV – Cost Variance

CVE – Common Vulnerabilities and Exposures

CVM – Critical Path Method

Calendar Unit – The smallest unit of time used in scheduling a project.

Campus – Buildings that share telecommunication facilities.

Capability – Aptitude, competency, or proven ability that is provided to the business or technical areas of an organization.

Capability Maturity Model (CMM) – A set of recommended practices in a number of key process areas that have been shown to enhance the capabilities of the software development organization. The CMM was developed for the federal government by the Software Engineering Institute (SEI) of Carnegie Mellon University.

Centralized Authentication and Authorization – A set of products based on directory services to store user credentials in a central directory.

Certificate Authority (CA) – Performs the management of certificates in a Public Key Infrastructure (PKI) implementation. A Certificate Authority maintains a highly secure environment to ensure master keys and certificate generation cannot be compromised.

Certificate-Based Authentication – Certificate-Based Authentication is the use of certificates to authenticate and encrypt traffic.

Challenge-Handshake Authentication Protocol (CHAP) – The Challenge-Handshake Authentication Protocol uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

Change – Modification to original specifications or alterations to achieve expected outcomes.

Change Control – A part of configuration management that reviews, approves, or tracks progress of alterations of a configuration item deliverable.

Change Control Board (CCB) – A formally constituted group of stakeholders responsible for approving or rejecting changes to the project baselines.

Change Management – The formal process of recording, analyzing, estimating, tracking and reporting of changes to the project baseline business functional requirements.

Change Management Plan – The formal, documented plan for managing change within the project.

Charter – A document issued by senior management that formally authorizes the existence of a project. A project charter provides the project manager with authority to apply organizational resources to project activities. (PMI)

Checkpoint – A point in the development process at which project state, status, and results are checked, recorded, and measured.

Cipher – A cryptographic algorithm for encryption and decryption.

Citizen – A resident of a city, town, or state entitled to vote and enjoy other privileges there.

Client – A piece of an application that the user sees and with which the user interacts. Clients can operate on many platforms including desktops, laptops, tablets, intelligent appliances, mobile computing devices, and electronic clipboards. It typically runs on an operating system that provides a GUI such as data or print services.

Client/server System – Traditionally a two-tier system with a relationship between processes running on two separate machines. A client initiates the dialog by sending requests to a server (or servers), according to some protocol, asking for information or action.

Closed Source – Software where the source code is kept private and concealed from the public view. Under most license agreements the user cannot modify or redistribute the program.

Cloud Access Security Broker (CASB) – A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to monitor all activity and enforce its own security policies. It can offer a variety of services, including but not limited to monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware.

Cloud Based Network Security Services – Cloud Based Network Security Services provide agencies and other government entities with customized access protection to/from their private networks. Firewall/VPN, Intrusion Prevention Services (IPS), and Secured Remote Access VPN are bundled together creating a complete security solution. By locating these services in the cloud, customers can protect multiple sites while utilizing only one security instance.

Cloud Computing – A model for enabling 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.

Cloud Service Provider (CSP) – An organization that provides cloud computing services.

Code Review – A formal meeting at which software code is presented and reviewed for approval by interested parties. (IEEE)

Coding – The transforming of logic and data from design specifications into a programming language. (IEEE)

Command and Control (C2, C&C) – Command-and-control servers issue commands and controls to compromised systems (often Internet-connected computers that then form zombie armies known as botnets). These communications can be as simple as maintaining a timed beacon or "heartbeat" so that the operators running the attack can keep an inventory of systems they have compromised within the target network, or use them for more malicious actions, such as remote control or data exfiltration. While the command-and-control server is used to control the system on the inside of the target organization, it is usually the compromised host that initiates the communication from inside the network to a command-and-control server on the public Internet.

Common Services and Integration Application – Common Services and Integration Applications are software programs, including databases, which support multiple business applications and/or facilitate integration and common use of data. Also called "Application Infrastructure."

Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme – As described in NIST SP 800-51, the Common Vulnerabilities and Exposures (CVE) vulnerability

naming scheme is a dictionary of common names for publicly known IT system vulnerabilities. It is an emerging industry standard that has achieved wide acceptance by the security industry and a number of government organizations. Technical vulnerability experts from 31 industry, academia, and government organizations vote on the common names. CVE provides the computer security community with the following:

- a comprehensive list of publicly known vulnerabilities;
- an analysis of the authenticity of newly published vulnerabilities; and
- a unique name to be used for each vulnerability.

General CVE information is available at https://cve.mitre.org.

Commercial Off-the-Shelf (COTS) – Hardware and software that can be purchased and put in service without additional development costs or a type of non-developmental software that is supplied by commercial sources.

Communications – Voice, video, and data capabilities that enable the leadership and staff to conduct the mission Essential Functions of the organization. Robust communications help ensure that the leadership receives coordinated, integrated policy and operational advice and recommendations and will provide the ability for governments and the private sector to communicate internally and with other entities (including with other Federal organizations, Tribal, State, Territorial, and local governments, and the private sector) as necessary to perform their Essential Functions. (FEMA)

Communications Management – The processes required to ensure the timely generation, collection, dissemination, storage, disposition, and disposal of project information.

Communications Management Plan – The formal document that defines communication management plans for the project.

Compatibility – The ability to run programs on multiple systems without alteration.

Components – Parts of a program or computer system.

Computer Aided Software Engineering (CASE) – Systems that attempt to automate some or all of the tasks involved in managing, designing, developing, and maintaining software systems.

Computer – An internally programmed automated device that performs data processing or telephone switching.

Computer Emergency Response Team (CERT) – An organization that studies computer and network Information Security (INFOSEC) in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Computer Security Incident – *See*, Cybersecurity Incident.

Computer System – At least one computer together with a set of related connected or unconnected peripheral devices.

Conceptual Architecture – *See*, Architecture Framework.

Confidence Level – A level of confidence, stated as a percentage, for a budget or schedule estimate. The higher the confidence level, the lower the risk.

Confidential Information – That information that is designated confidential by law, including certain health information, tax records, and personal information.

Confidential Information Technology Security Records – Those information technology security records designated as confidential by an agency pursuant to N.C.G.S 132-6.1(c).

Confidentiality – Written communication conducted in confidence of secrecy, as authorized by State and federal laws.

Configuration – The arrangement of a computer system as defined by the number, nature, and interconnections of its constituent parts. (IEEE)

The functional and physical characteristics of hardware or software as set forth in technical documentation or achieved in a product. (IEEE-STD-610)

Configuration Management – Methodical storage and recording of all software components and deliverables during development. The process of identifying and defining the baseline items in a system, controlling the release and change of these items, and recording and reporting the status of baseline items and change requests.

Configuration Management Plan – A record that documents what software configuration management activities are to be done, how they are to be done, who is responsible for doing specific activities, when they are to happen, and what resources are required. (IEEE)

Configuration Management System – The process, procedures, and tools used by the development organization to accomplish the configuration management requirement.

Confirmation – The act of validating a security incident through procedures established by the agency that conform to best practices.

Connectivity – The ability to send and receive information between locations, devices, and business services. Usually associated with the degree to which nodes and networks are connected.

Consent Banner – A statement that pops up when a user attempts to access an electronic information system such as an Internet page or a telnet site. The banner contains a message requiring an acceptance of the terms and conditions before the user accesses the page.

Consistency – The degree of uniformity, standardization, and freedom from contradiction among the documents or parts of a system or component. (IEEE)

Constraint – Boundaries, restrictions, limitations, or obstructions to the successful completion of a project.

Continuity – An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event. (FEMA)

Continuity Facilities – Continuity facilities is comprehensive term and refers to both Continuity and Devolution sites where Essential Functions are continued or resumed during a Continuity event. Alternate sites are locations, other than the primary facility used to carry out Essential Functions by relocating ERG members following activation of the Continuity Plan. Devolution sites are locations used to carry out Essential Functions by devolving the Essential Functions to a geographically separated facility and staff (the DERG) following activation of the devolution plan. These sites refer to not only other facilities and locations, but also work arrangements such as telework and mobile work concepts. (FEMA)

Continuity of Government (COG) – The preservation, maintenance, or reconstitution of civil government's ability to carry out the executive, legislative and judicial processes under the threat or occurrence of any emergency condition that could disrupt such processes and services.

Continuity of Government Readiness Conditions (COGCON) – For the Federal Executive Branch, the COGCON system establishes readiness levels in order to provide a flexible and coordinated response to escalating threat levels or actual emergencies, focusing on possible threats to the National Capital Region. The COGCON system establishes, measures, and reports the readiness of executive branch Continuity programs, which is independent of other Federal Government readiness systems. (FEMA)

Continuity of Operations (COOP) – The ability to recover and provide services sufficient to meet the minimal needs of users of the system/agency. This ability to continue essential agency functions across a wide spectrum of emergencies will not necessarily limit COG functions.

Continuity Manager – The senior Continuity planner who manages day-to-day Continuity programs, represents their department or agency on the Continuity Advisory Group and working groups, as appropriate, and reports to the Continuity Coordinator on all Continuity program activities. (FEMA)

Continuity Personnel – Those personnel, both senior and core, who provide the leadership advice, recommendations, and functional support necessary to continue essential operations. Continuity personnel are referred to as ERG members. (FEMA)

Continuity Plan – A plan that details how an individual organization will ensure it can continue to perform its Essential Functions during a wide range of emergencies. (FEMA)

Continuity Program Management Cycle – An ongoing, cyclical model of planning, training, evaluating, and implementing corrective actions for Continuity capabilities. (FEMA)

Continuous Diagnostics and Mitigation (CDM) – A dynamic approach to fortifying the cybersecurity of networks and systems. CDM provides organizations with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Continuous Monitoring – Continuous monitoring of information systems is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This involves collecting and analyzing information regularly from multiple sources in accordance with pre-established metrics in order to manage risk as appropriate for each organizational tier.

Contract – A mutually binding agreement that obligates the seller to provide a specified product or service and obligates the buyer to pay for it. Contracts may be either: fixed price (lump sum contracts), cost reimbursable, or unit price. (PMI)

Contract Administration – Monitoring and control of performance, reviewing progress, making payments, recommending modifications, and approving contractor / supplier actions to ensure compliance with contractual terms during contract execution.

Control – A process for assuring that reality, or actual performance, meets expectations or planned performance.

Conversion – To change one system or data to another system.

Cooperative Processing – Computing that requires two or more distinct processors to complete a single transaction.

Copyleft – A term coined for the application of copyright law to ensure public freedom to manipulate, improve, and redistribute a work of authorship and all derivative works. The copyright holder grants an irrevocable license to the recipient of a copy, permitting the redistribution (including sales) of possibly modified further copies, under the condition that all those copies carry the same license and are made available in a form, which facilitates modification.

Core Business Application – An application with the following attributes: A user interface visible to and directly used by the end users which can support more than one user to add/delete/create information at the same time, and is server/mainframe based, sharing data, via interfaces, with other applications.

Corrective Action – Changes made to bring expected future performance of the project in line with the plan. (PMI)

Corrective Action Plan (CAP) - A corrective action plan (CAP) is a step by step plan of action and schedule that is developed to correct a process or area of non-compliance, that often includes the most cost-effective actions that can be implemented to correct errors.

Corrective Action Program (CAP) – An organized method to document and track improvement actions for a program. (FEMA)

Corrective Maintenance – Maintenance performed to correct faults in hardware or software. (IEEE)

Cost / Benefit Analysis – A formal study in which the development, execution, and maintenance costs for a project are matched against the anticipated value of the product.

Cost Estimating – Developing an approximation (estimate) of the cost of the resources needed to complete the project. (PMI)

Cost Performance Index (CPI) – The ratio of budgeted costs to actual costs (BCWP/ ACWP) used to predict potential cost overrun – original cost estimate / CPI = projected cost at completion.

Cost Variance (CV) – Difference between the estimated cost of an activity and the actual cost of an activity.

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) – The preferred encryption protocol in the 802.11i standard.

Coverage Testing – Testing to ensure that all lines of code are exercised.

Credentials – Within information systems, electronic credentials are a means to identify people and resources and control their access to information systems and data. A widely used form of electronic credentials is a combination of a user account number or name and a password or Personal Identification Number (PIN). Other forms of electronic credentials include fingerprints, voice recognition, retinal scans, facial recognition systems, and digital certificates.

Criminal Justice Information (CJI) – Criminal Justice Information is Criminal Justice Information System (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets:

- Biometric Data – data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from

within a population. This data is used to identify individuals, to include fingerprints, palm prints, iris scans, and facial recognition data.

- Identity History Data – textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
- Biographic Data – information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
- Property Data – information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
- Case/Incident History – information about the history of criminal incidents.

Critical Activity – A task, activity, or event that, if delayed, will delay another important event - probably the completion of the project or a major milestone in the project. Any activity on the critical path.

Critical Application / Function – An application, activity or business function that, if unavailable, would negatively impact an agency's timely delivery of critical automated business services to the state's citizens. *See,* Application Criticality.

Critical Data Point – *See,* Recovery Point Objective.

Criticality – The quality, state, or degree of being of the highest importance.

Critical Design Review – Phase transition review for exit of the high-level design phase and entry into the detail design phase.

Critical Path – Derived from the PERT method, this term implies the set of activities that must be completed in sequence and on time if the entire project is to be completed on time. A missed task on the critical path will cause a product delivery delay.

Critical Path Method (CPM) – A scheduling technique using the precedence diagrams to determine the length of a project based on the end-to-end tasks that are critical to the completion of a project. One of the two most common forms of networking systems. CPM uses a one-time estimate for creating a project schedule.

Critical Success Factors – Objectives, goals, and conditions required for a project to demonstrate success.

Cryptography – A technology that scrambles data to prevent unauthorized individuals from reading the data. A cryptographic key is a sequence of numbers and characters used in scrambling and unscrambling the data.

Current Finish Date – The current estimate of the point in time when a task or activity will be completed.

Current Start Date – The current estimate of the point in time when a task or activity will begin.

Customer – The individual or organization that specifies the product specifications (requirements) and formally accepts the project deliverables or the person or organization receiving the product or service.

Cyber Crime – A criminal act involving computers or computer networks. Cyber crimes can be comprised of cyber attacks such as stalking and distribution of viruses and other malicious code or traditional crimes (e.g. bank fraud, identity theft, and credit card account theft).

Cyber Attack – An act, usually through the Internet, that attempts to undermine confidentiality, integrity, or availability of computers or computer networks, or the information that resides within the systems themselves. A cyber attack is sometimes referred to as hacking.

Cyber Breach – *See*, Breach.

Cybersecurity Incident – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. A Cybersecurity Incident is an **adverse** event where an information technology resource is accessed or used without authorization, attacked or threatened with attack, or used in a manner inconsistent with established policy with the potential to cause the real or possible loss of confidentiality, integrity, or availability of the resource or its information.

Examples of information technology incidents are as following:

- Unauthorized attempts (either failed or successful) to gain access to a State-owned/operated/managed system or its data.
- Unauthorized or misuse of a system for the processing or storage of data.
- Intentional or unintentional disruption of processing capability or denial of service (DoS) attacks.
- Actual or suspected loss of proprietary or entrusted information.
- Using information systems to commit financial crimes or cause financial loss to the State or the citizens of North Carolina.
- Changes to system hardware, firmware, or software configurations without appropriate agency approval.
- Malicious logic (virus, worm, Trojan horse) attacks.
- Attempted or actual instances of social engineering.
- Perpetration of hoaxes.

- Copyright violations.
- Unauthorized network scans or probes.

Examples of incidents or events that are not information technology security incidents are:

- Spam
- Virus attacks that are blocked through software operating at the agency
- Events that are blocked through intrusion prevention programs
- Adverse Weather Conditions
- "Normal" or expected system crash (Windows Blue Screen)
- Money scams (like Nigerian money scam, credit card requests)

D

DAC – Discretionary Access Control

DDoS – Distributed Denial of Service

DES – Data Encryption Standard

DHS – Department of Homeland Security

DIT – Department of Information Technology

DMZ – Demilitarized Zone

DoS – Denial of Service

DNS – Domain Name System

DSA – Digital Signature Algorithm

DSS – Digital Signature Standard

Daemon – A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term. At the same time, many other operating systems provide support for daemons, although daemons may be called something else. Windows, for example, refers to daemons, System Agents, and services.

Dashboard – A chart that provides visual graphs and instant insight into an individual technology investment, a group of investments or a specific criterion. Enables managers to focus in on key performance indicators and trends critical to their specific areas of interest and responsibility.

Data – The State's information assets converted into a binary digital form that can be digitally transmitted or processed. The numbers, text, graphics, images, and voice stored in a form that can be used by a computer.

Data Access Audit – A review of network traffic connection data collected on networks. The data typically consist of summarized connection records (date, time, source and destination address, source and destination port) along with daily summary statistics depicting the summary of connections by service (or port) and local and remote addresses.

Data Breach – *See*, Breach.

Database – A collection of data elements structured into one or more large sets of data.

Data Center – A dedicated, secure facility that houses systems components with the necessary power, bandwidth, and support services to ensure system availability.

Data Dictionary – A centralized repository of information about data (e.g., meaning, origin, usage, format, relationship to other data elements). A file that defines the organization of a database.

Data Domain – *See*, Statewide Architecture Framework.

Data Encryption Standard (DES) – A widely used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. The stronger Triple DES method, or 3DES, is used in many newer systems.

Data Flow Diagram – A picture diagramming how data flows through a system.

Datagram – A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network. The term has been generally replaced by the word packet.

Data Leak Prevention – In data leakage incidents, sensitive or confidential data is disclosed to unauthorized personnel either accidentally or maliciously. Data loss incidents become data leak incidents when sensitive information is lost and subsequently acquired by an unauthorized party. A data leak is possible without the data being lost on the originating side. *See*, Data Loss Prevention.

Data Loss Prevention – A strategy to classify and protect sensitive or confidential information so end users cannot accidentally or purposely share that data outside the organization's network. In addition to being able to monitor and control endpoint activities, some DLP

solutions can also filter data on the network and protect data in motion. The terms “data loss” and “data leak” are closely related and are often used interchangeably, though they are somewhat different. *See*, Data Leak Prevention.

Data Spillage – The transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications, or media. A spillage can be from a higher level classification to a lower one.

Data Standards – Agreed upon terms for defining and sharing data.

Data Store – A place where data, including archived data, are stored.

Data Warehouse – A process by which operational data are transformed, stored, managed, and delivered for decision support systems.

Debugging – The process of correcting syntactic and logical errors detected during coding.

Decision Trees – Branching chart depicting the actions that occur from various combinations of decisions or conditions.

Decryption – The process of transforming an encrypted message into its original plain text.

Defect – A flaw in a system that causes the system to fail to perform as required.

Defense in Depth – A security approach that uses multiple layers of security to guard against failure of any single security component.

Degauss – To remove or neutralize the magnetic field of a magnetic tape, hard drive or floppy disk by applying a decaying and alternating magnetic field.

Delegation of Authority – Delegations of Authority are formal documents that specify the activities that those who are authorized to act on behalf of the agency head or other key officials may perform. Delegations of authority document the legal authority for officials—including those below the agency head—to make key policy decisions during a COOP situation. (FEMA)

Deliverable – Any unique and verifiable product, result, or capability to perform a service that must be produced to complete a process, phase, or project. Often used more narrowly in reference to an external deliverable, which is a deliverable that is subject to approval by the project sponsor or customer. (PMI)

Demilitarized Zone (DMZ) – A section of the network that is inserted as a "neutral zone" between an organization’s internal private network and the outside public network. A DMZ prevents outside users from gaining direct access to the servers and resources in the secure zone of the organization’s network.

Denial of Service (DoS) – An incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail to be available or the temporary loss of all network connectivity and services.

Department Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to this department's core functions, processes and/or activities.

Department of Homeland Security (DHS) – A federal agency that was created through the integration of all or part of twenty-two different federal departments and agencies into a unified, integrated department whose mission is to secure the nation from the many threats we face.

Department of Information Technology (DIT) – DIT is a Cabinet-level department under the direction of the State Chief Information Officer. DIT is a major provider of information technology services, such as computing, security and telecommunications, to other governmental agencies. It must take appropriate steps to protect the state's information assets within its control and to establish statewide information technology security standards.

Dependency Diagram – Another name for a network or precedence diagram that shows the dependencies among tasks.

Design – The focus on the applications and technology required to support the current and future business process. It could also be the tasks associated with specifying and sketching the features and functions of a new application prior to coding.

Design Pattern – A written document that describes a general solution to a design problem that recurs repeatedly in many projects.

Design Specification – A document that prescribes the form, parts, and details of the product.

Desktop Computer – A desktop computer is a personal computer (PC) intended for regular use at a single location desk/table due to its size and power requirements. The most common configuration includes a computer monitor, keyboard and mouse, and a case that houses the main components of the PC.

Desktop Application – Applications or individual productivity applications that support one or few users and are based on commonly available tools like Microsoft Word or Microsoft Excel.

Desktop and Handheld Device Encryption – Software products designed to protect data kept in files or databases on a local network drive.

Development Process – The process for managing the development of the defined product. Usually involves the implementation of a defined System Development Life Cycle (SDLC).

Development Project – The sum of all tasks and activities necessary to build a software product. Development projects provide new functionality or enhanced functionality to a new or existing application system.

Development System – The hardware and software tools and supporting equipment (e.g., operating systems, compilers, browsers) that will be used in software development.

Devolution – Devolution requires the transition of roles and responsibilities for performance of Essential Functions through pre-authorized Delegations of Authority and responsibility. The authorities are delegated from an organization's primary operating staff to other employees internal or external to the organization in order to sustain Essential Functions for an extended period. Devolution is a Continuity option instead of or in conjunction with relocation in order to ensure the continued performance of Essential Functions. (FEMA)

Devolution Emergency Relocation Group – Personnel stationed at the devolution site who are identified to conduct Essential Functions. (FEMA)

Devolution Site – "Devolution sites" are locations used to carry out Essential Functions by devolving the Essential Functions to a geographically separated facility and staff (the DERG) following activation of the devolution plan. These sites refer to not only other facilities, but also work arrangements such as telework and mobile work concepts. (FEMA)

Diffie-Hellman – A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digital Certificate – A digital certificate is an electronic unit that establishes your credentials when doing business or other transactions. It is issued by a certificate authority. It contains the owner's name, a serial number, expiration dates, a copy of the certificate holder's public key (public keys verify signatures, private keys are used to create them), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

A digital certificate is an electronic document that binds an individual with his public encryption key.

In electronic communications, there must be some means to verify a public key and its owner in place of face-to-face and photo-id verification. One way is through the use of a trusted electronic record called a digital certificate. The digital certificate is issued by a trusted third-party who has vouched for the claimant's identity and public key. A certificate contains the owner's name, owner's public keys, an expiration date, the third-party's digital signature and other information. The certificate is considered reliable because it is digitally signed by a trusted authority. A recipient can always authenticate a digital certificate by applying the trusted authority's public key to the digital signature and comparing the recovered information with the certificate contents. The trusted authorities that issue certificates are known as Certificate Authorities.

Digital Signature – A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission. A digital signature is a piece of electronic information that links the original message content that was signed with the identity of the signer. A digital signature can provide the same functionality as a handwritten signature because it ties an individual to an original document.

The first step in digitally signing an electronic document is to generate a message digest of the document. Next, the signer encrypts this message digest using the signer's private key. The resulting encrypted message digest is called a digital signature. Then the document and digital signature are sent to one or more recipients. The process is reversed to verify a digital signature. First, the recipient recovers the original message digest from the digital signature by using the signer's public key to decrypt the message digest. Next, the recipient generates a message digest from the original document. Finally, the recipient compares the generated message digest with the recovered message digest. If the recovered and the generated message digests are equal, then the recipient is assured that the document has not been modified.

The identity of the sender is assured, since the public key of the sender was used to recover the original message digest that was encrypted with the sender's private key. The digital signature, therefore, provides *non-repudiation*, which means that the sender cannot deny having sent the message.

Digital Signature Algorithm (DSA) – An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Digital Signature Standard (DSS) – The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

Directory Services – A database that provides a central point for authentication (log-in) and a view of all available resources on the network, as well as facilitating authorization (access control), navigation of the networks, and communication among current and future systems.

Disaster Recovery Plan – A tactical plan that defines the information technology resources, actions, tasks, and data required to successfully recover critical business processes and minimize the impact of damage caused by a disaster. The Disaster Recovery Plan is used to restore essential business processes and ensure that the state's critical information assets remain available during a disaster according to predetermined Business Continuity Plan goals and objectives. A disaster can be defined as any event that places the integrity of the state's information assets in question or renders it inaccessible.

Discretionary Access Control (DAC) – A method that restricts user access rights to objects based on the identity or needs of the user. Usually, the controls are put in place by the system administrator. The controls are discretionary in that a subject with certain access permission is

able to pass that permission (directly or indirectly) to any other subject. This is the most common type of access control.

Disruption – The interruption of information availability or access.

Distributed Computing Environment – a computing environment that may involve multiple computers, often of differing architectures and data representation formats that share data and system resources. A distributed computing environment is usually managed as a large, single entity.

Distributed Denial of Service (DDoS) – An incident in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Distributed Network – A computer network on which processing is shared by many different parts of the network. Processing may be shared by client (local) computers, files servers, print servers, application servers, and database servers.

Distributed Processing – A technique that allows multiple computers on a network to share the work between them. In contrast to mainframe operations, distributed processing enables more efficient allocation of processing power because available processors can be used as either general or job-specific processors, depending on the type of work to be done, the existing workload, and the capabilities of the various processors.

Document of Understanding – A formal agreement between two parties that is sometimes referred to as a Statement of Work (SOW).

Documentation – The printed and displayed materials that explain an application to a user. Any written or pictorial information annotating, describing, defining, specifying, reporting, or certifying activities, requirements, procedures, results, or products.

Domain Name System (DNS) – The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain Name System (DNS) Zone – A part of the DNS tree that is treated as a unit and contains data used to map addresses to names.

Domain Name System (DNS) Zone Transfer – *See*, Zone Transfer.

Downward Compatible – Pertaining to hardware or software that is compatible with earlier versions of itself.

Drive-Away Kit – A kit prepared by, and for, an individual who expects to deploy to an alternate site during an emergency. The kit contains items needed to minimally satisfy an individual's personal and professional needs during deployment, such as clothing, medications, a laptop, and other necessities. Also referred to as a 'To-Go Kit." (FEMA)

Dynamic Link Library – A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

E

EA – Enterprise Architecture

EAC – Estimate at Complete

eBusiness – Electronic Business

eCommerce – Electronic Commerce

EDC – Eastern North Carolina Data Center

EGRC – Enterprise Governance, Risk, and Compliance

EI-ISAC – Elections Infrastructure Information Sharing & Analysis Center

E-mail – Electronic Mail

EV – Earned Value

ETA – Enterprise Technical Architect

ETC – Estimate to Complete

EWTA – Enterprise-Wide Technical Architecture

Earned Value (EV) – A method for measuring project performance by comparing the amount of work that was planned with what was actually accomplished to determine if cost and schedule performance are as planned.

Effectiveness – A measure of the quality of attainment in meeting objectives.

Efficiency – A measure of the volume of output received for the input used.

Elapsed Time – The time passed before the measuring takes place. It can be measured using labor hour or calendar day.

Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) – The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) was established by the EIS-GCC to support the cybersecurity needs of the elections subsector. Through the EI-ISAC, election agencies will gain access to an elections-focused cyber defense suite, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices.

Electronic Business (eBusiness) – The process of not only selling goods and services, but also of servicing customers and collaborating with business partners.

Electronic Commerce (eCommerce) – The purchase and distribution of goods and services across the Internet.

Electronic Storage Media – Materials used to store data in electronic form, including floppy disks, magnetic tape, CD-ROMs and computer hard drives.

Electronic-Mail (E-Mail) – The capability to compose, address, and send messages electronically.

Emergency Operating Records – Records that support the execution of an organization's Essential Functions. (FEMA)

Emergency Relocation Group – Staff assigned responsibility to continue Essential Functions from an alternate site in the event that their primary operating facilities are threatened or have been incapacitated by an incident. (FEMA)

Encapsulation – The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

Encapsulation Security Payload (ESP) – Sender authentication, integrity, and confidentiality. *See,* Internet Protocol Security (IPSec).

Encryption – The conversion of data into a form that cannot be readily understood by unauthorized people, to ensure that only the intended recipient is allowed to read the data. The term applies to both data in transit (communications) and stored data.

> **Container-based Encryption** provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields.
>
> **Full Disk Encryption** is performed at the disk sector level encrypting all information stored on a disk. When configured properly, Full Disk Encryption prevents unauthorized

access to information by decrypting information only after successful authentication. All information on a protected disk including all operating system, swap files, temporary files, applications, data files and unallocated sectors are encrypted.

Endpoint – Endpoint or end point is a physical device, such as a laptop, desktop or mobile device, which connects in some manner (physically, wirelessly, or remotely) to a network. An end point is the primary physical device through which users interface with the local applications as well as network delivered resources. Once an endpoint is connected it becomes a point of termination on a network. As with other points on a network, an end point may increase risk to the security of the network.

Enhancement – A change to an application, which is intended to increase functionality, improves performance, and/or adds additional capability.

Enterprise – All state agencies, departments, institutions, commissions, committees, boards, divisions, bureaus, offices, officers, and officials of the State. The term does not include any State agency excluded from coverage under this Article by G.S. § 143B-1300, unless they elect to participate in the information technology programs, services, or contracts offered by the Department of Information Technology (DIT).

Enterprise Architecture (EA) – A set of design principles consistently applied across the organization that guides the development and implementation of information systems and technology infrastructure. The Enterprise Architecture is a disciplined process that details the enterprise's technology strategies, its extended technology linkage, and the impact on program and project initiatives. Enterprise Architecture consists of four separate subordinate architectures: Enterprise Business Architecture (EBA), Enterprise Information Architecture (EIA), Enterprise Solution Architecture (ESA), and Enterprise Technical Architecture (ETA).

Enterprise Governance, Risk, and Compliance (EGRC) – An enterprise approach to automating the management, measurement, remediation and reporting of controls and risks against stated objectives, in accordance with state laws, policies, standards and business requirements.

Enterprise Planning – The process of developing business, program and technology strategic directions and policies from a statewide perspective. State technology strategy is accomplished by synchronizing Information Technology plans and technology investments with statewide governmental initiatives, agency goals and objectives, and business or program requirements.

Enterprise System Management Domain – *See,* Statewide Architecture Framework.

Enterprise Technical Architect (ETA) – An individual primarily focused on the development of technology principles, practices, and standards that are highly leverageable across multiple solutions. The Enterprise Technical Architect provides the bridge between the deeply technical domain architects and the business analysts to ensure the technology infrastructure meets the goals of extensibility and complexity reduction.

Enterprise-Wide Technical Architecture (EWTA) – *See,* Statewide Architecture Framework.

Entity – An organization (as a business or governmental unit) that has a legal identity.

Environment – The set of tools and physical surroundings in which software is developed.

Error – A fault or discrepancy between what is computed and what is true.

Essential Functions – Essential Functions are a subset of government functions that are determined to be critical activities. These Essential Functions are then used to identify supporting tasks and resources that must be included in the organization's Continuity planning process. In this FCD, the term "Essential Functions" refers to those functions an organization must continue in a Continuity situation, whether the functions are MEFs, PMEFs, or Essential Supporting Activities. (FEMA)

Essential Records – Information systems and applications, electronic and hardcopy documents, references, and records needed to support Essential Functions during a Continuity event. The two basic categories of essential records are emergency operating records and rights and interest records. Emergency operating records are essential to the continued functioning or reconstitution of an organization. Rights and interest records are critical to carrying out an organization's essential legal and financial functions and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. The term "vital records" refers to a specific sub-set of essential records relating to birth, death, and marriage documents. (FEMA)

Essential Records Plan Packet – An essential records plan packet is an electronic or hard copy compilation of key information, instructions and supporting documentation needed to access essential records in an emergency situation. (FEMA)

Estimate – A predicted total of expenditures required to complete a task, activity, or project. An approximate judgment of the effort, cost, or time scale to perform a specified piece of work.

Estimate at Complete (EAC) – The expected total cost of a task or activity when the defined scope of work has been completed.

Estimate to Complete (ETC) – The expected additional cost of an activity when the defined scope of work has been completed.

Evergreen Strategy – A plan for the continued maintenance of the North Carolina Statewide Architecture Framework.

Evolutionary Development Model – A system development life cycle approach whose stages consist of expanding increments of an operational software product. (Sometime called evolutionary prototyping.)

Exception Process – An acknowledgement or request for an agency to proceed contrary to an established law, policy, or standard practice. Exceptions can be for procurement, security or standards and they require DIT or State CIO reporting and/or approval.

Exit Criteria – The set of conditions that must be met prior to completing a project phase or application.

Exploit – An attack that takes advantage of vulnerabilities in an application, operating system (OS), network, or hardware. Exploits usually take the form of software or code that aim to gain control of computers or steal data.

Extensible – Describes an architecture that allows new technology to be added, as required by business conditions.

External Access Control – A means of controlling interactions between enterprise resources and outside people.

External Connections – Any physical connection to devices, other than its main connection to the network. A unidirectional connection from a higher security zone to a lower security zone is not considered an external connection. Examples of external connections include dial-up modems on servers, etc.

External Dependency – Any deliverable product or service from other organizations that may be critical to the project.

External Interface – The point where the software system interacts with other software systems, products, or people.

Extranet – A secure extension of a private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

F

FedRAMP – Federal Risk and Authorization Management Program

FEMA – Federal Emergency Management Agency

FERPA – Family Educational Rights and Privacy Act

FIPS – Federal Information Processing Standard

FTI – Federal Tax Information

FTP – File Transfer Protocol

Failure - A malfunction of a user's installation. It may result from a bug, incorrect installation, a communication line hit, a hardware failure, and so forth.

Failure Rate – The ratio of the number of failures of a given category to a given unit of measure. (IEEE)

Family Educational Rights and Privacy Act (FERPA) – The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Schools may disclose, without consent, directory information identified below, however, the schools must inform parents and eligible students about directory information and allow for parental and eligible students to opt out of the disclosure.

- Student name
- Student address
- Student telephone number
- Date and place of birth
- Honors and awards
- Dates of attendance

Fast Tracking – Compressing the project schedule by overlapping activities that would normally be done in sequence (e.g., design and construction). (PMI)

Fat Client – The term used when most of a two-tier application runs on the workstation. Fat client applications access database and file servers. Fat client applications are inflexible, difficult to change when business requirements change, and difficult to manage. A fat client application is essentially a monolithic application that accesses data stored on a server.

Fault – An incorrect step, process, or data definition. (IEEE)

Feasibility – The degree to which the requirements, design, or plans for a system can be implemented under existing constraints. (IEEE)

Feature – A distinguishing characteristic of a software item. (IEEE)

Federal Emergency Management Agency (FEMA) – A federal agency that coordinates the federal government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. FEMA's mission is to lead America to prepare for, prevent, respond to and recover from disasters with a vision of "A Nation Prepared".

Federal Information Processing Standards (FIPS) – Standards developed by NIST that address computing within federal agencies only when no voluntary standards address federal

requirements for the interoperability of different systems, for the portability of data and software, and for computer security. Subjects include encryption.

Federal Continuity Directive (FCD) – A document developed and promulgated by DHS, in coordination with the Continuity Advisory Group and in consultation with the Continuity Policy Coordination Committee, which directs executive branch organizations to carry out identified Continuity planning requirements and assessment criteria. (FEMA)

Federal Risk and Authorization Management Program (FedRAMP) – A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Federal Tax Information (FTI) – FTI is any tax return or tax return information received from the IRS or secondary source, such as the Social Security Administration (SSA), the Federal Office of Child Support Enforcement, or the Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from a return or return information. FTI may include some PII elements.

Feedback – Information from some process that is sent back.

File – A named set of records.

File Transfer Protocol (FTP) – A TCP/IP protocol specifying the transfer of text or binary files across the network. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

Filtering – A process to screen access to locations or information content on a selective basis. It can include blocking words and images, hosts, sites, or protocols from access on a specific information technology system or an individual computer. Filtering may be performed on a selective basis. Keyword blocking targets words or strings of words to be blocked from access. Host blocking means that specific Internet sites are selected for blocking. Protocol filtering means blocking access to entire applications such as Usenet and FTP.

Financial Close Out – Accounting analysis of how funds were spent in achieving a project.

Finish Date – The point in time associated with task or activity completion.

Firewall – A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. Central point of control for regulating traffic flow between internal and external "untrusted" networks. It is also a term used for software or devices used to control access from one network, usually external, to another internal network.

Firewall Ruleset – A table of instructions that the firewall uses for determining how packets should be routed between its interfaces. In routers, the ruleset can be a file that the router examines from top to bottom when making routing decisions.

Firmware – Hardware that contains a computer program or data that cannot be changed in the user environment.

Fix – A Patch.

Flexibility – The ease with which a system can be modified for use in other environments. (IEEE)

Float – The amount of time for a task to be freely scheduled without affecting other tasks in the project. (PMI)

Flowchart – A graphical representation of a process.

Forecasting – The management process of attempting to predict future events.

Formal Inspections – In-process technical reviews of a product of the software development life cycle conducted for the purpose of finding and eliminating defects.

Formal Testing – Testing conducted in accordance with documented test plans and procedures. (IEEE)

Form-Based Authentication – Form-Based Authentication uses forms on a webpage to ask a user to input username and password information.

Free Software – Free software is software that can be freely used, modified, and redistributed. However, any redistributed version of the software must be distributed with the original terms of free use, modification, and distribution. Licenses may contain "copyleft" restrictions requiring the source code to always be made available and that derived products must be released under the exact same license. The Free Software Foundation definition of free software is stipulated as part of the GNU project. Unlike freeware, free software may be distributed for a fee.

Freeware – Freeware (not to be confused with free software) is software that is offered at no cost and is a common class of small applications available for download. Typically, freeware does not provide the source code and is often covered under copyright and licensing agreements.

Full Disk Encryption – *See*, encryption

Function – An activity that spans the entire duration of a software project (e.g., status reporting, quality assurance, verification and validation).

Function Point – A measurement of the functionality of the software product in standard units independent of the coding language.

Function Testing – A part of systems testing that confirms that the application meets the user business requirements.

Functional Decomposition – Modular decomposition in which a system is broken down into components that correspond to system functions and sub-functions. (IEEE)

Functional Design – The process of defining the working relationship among the components of the system. (IEEE)

Functional Requirement – A requirement that specifies a function that a system must be able to perform. (IEEE)

Functional Specification – The formal description of a software system that becomes the blueprint for implementation.

G

GLB – Gramm-Leach-Bliley Act

GNU – Gnu's Not Unix

GPL – General Public License

GUI – Graphical User Interface

Gantt Chart – A method of displaying overlapped and partially concurrent activities by using horizontal lines to reflect the time required by each activity. The chart, named for Henry Lawrence Gantt, consists of a table of project task information and a bar chart that graphically displays the project schedule to be used in planning and tracking. *See,* bar chart.

Gap Analysis – A format used to clarify the relationship between two factors.

Gate – Review at the end of a life cycle phase.

Gateway – A network point that acts as an entrance to another network.

General Public License (GPL) – This is also referred to as the "GNU GPL." The GPL was written in 1987 for use with programs released as part of the GNU project. It was based on a combination of similar licenses used for early GNU projects. The goal was to produce one license that could be used for any project, thus making it possible for many projects to share code. Since its introduction, it has become the most widely used free software license. As of January 2004, the most current version of the GNU GPL is version 2, which was released in 1991. Version 3 is in development.

Goal – A strategic objective designed to provide a target for achievement through the attainment of enabling objectives.

Government Functions – Government functions are the collective functions of organizations, as defined by the Constitution, statute, regulation, presidential direction or other legal authorities, and the functions of the legislative and judicial branches. These functions are activities that are conducted to accomplish an organization's mission and serve its stakeholders. (FEMA)

Gramm-Leach-Bliley Act (GLB) – Financial Services Modernization Act, Public Law 106-102, signed 1 November 1999. The Act legislates broad requirements for financial services and insurance providers. Section V of the Act deals with privacy and security requirements.

Granular – A term describing the art of writing small modules of code and/or objects. Dividing a program into very small modules is advantageous because an individual module can be modified to support changing business requirements without impacting the rest of the program and because granular modules facilitate software component re-use.

Graph – A diagram that represents the variation of a variable in comparison to other variables.

Guideline – A best practice for agencies to use when implementing a policy until a standard is developed.

H

HIPAA – Health Insurance Portability and Accountability Act of 1996

HSEEP – Homeland Security Exercise and Evaluation Program

HTML – Hypertext Markup Language

Hacker – 1) One who uses programming skills to gain illegal access to a computer network or file; 2) One who is proficient at using or programming a computer.

Hacking – 1) The breaking into computer systems or files using programming skills. Hacking may be performed for the pleasure/fun of it without the motivation for financial gain; 2) The hobby/profession of working with computers.

Hardcoded – An informal term that describes a programming technique where data, directions, procedures and passwords are specifically written into the program instructions. This technique results in static, inflexible systems that require intensive labor to maintain the program.

Hardware – Physical equipment used to process, store or transmit, computer program data.

Hardware Specification – The functions, materials, dimensions, and workmanship that a hardware item must satisfy.

Hash – A number generated from a string of text. The hash is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same has value. Hashes play a role in security systems where they are used to ensure that transmitted messages have not been tampered with.

Health Insurance Portability and Accountability Act (HIPAA) – HIPAA (Public Law 104-191, also known as the Kennedy-Kassenbaum Bill) is a federal law that includes specific requirements to maintain the privacy and security of "protected health information." HIPAA data applies to any data from a Covered Health Care Provider, Health Care Clearing House, or Health Information that is created, transmitted, stored or received. It also includes code sets, health plans and Individually Identifiable Health Information. This can include, demographic information collected that is not limited to the following:

- Health data created by a health care provider, health plan, employer, or health care clearinghouse;
- Identified the individual;
- Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Heterogeneous Networking – The networking of computers from different vendors, or the running of different operating systems.

Hierarchy – A structure in which components are ranked into levels of subordination. (IEEE)

Homeland Security Exercise and Evaluation Program (HSEEP) – A Department of Homeland Security (DHS) program that provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.

Host Based Intrusion Detection - *See,* Intrusion Detection

Hosting – A service in which an application service provider houses an application and support the hardware and software needed to operate an information technology application.

Human Factors – The characteristics, limitations, physical requirements, and psychological needs of people that must be considered in the design and development of a system.

Hyperlink – A link within a document that leads to another site, or another place within the same document. Hyperlinks are usually underlined or shown in a different color from the surrounding text.

Hyper Text Markup Language (HTML) – The language used to convert text documents into online help and Web pages.

Hypervisor / Host OS – a virtualization platform that allows multiple operating systems to run on a host computer at the same time. Also called a Virtual Machine Host or Virtual Machine Monitor.

I

ICMP – Internet Control Message Protocol

IEEE – Institute of Electrical & Electronic Engineers

IFB – Invitation for Bid

IKE – Internet Key Exchanges

IOA – Indicators of Attack

IOC – Indicators of Compromise

IoT – Internet of Things

IP – Internet Protocol

IPSec – Internet Protocol Security

ISO – International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

IV & V – Independent Verification and Validation

Identification – The assignment of a name by which an entity can referenced. The entity may be high level such as a human user or low level such as a process or communication channel. The process of distinguishing one user from all others.

Identity – Identity is who someone or what something is, such as the name by which something is known.

IEEE 802.1X – An authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the network until it provides

credentials, like a user name and password, that are verified by a separate server. In 802.1X, there are three roles: the supplicant (client), authenticator (switch or access point), and authentication server.

Implementation Guidelines – A Statewide Architecture Framework complementary architectural component that provides best practices with discussion regarding implementation issues and associated resolutions for the eight technical architectural domains.

Implementation Phase – Preparing the product for use by the customer.

Incremental Development – Software development technique in which requirements definition, design, implementation, and testing occur in an overlapping, iterative manner resulting in incremental completion of the project. (IEEE)

Independent Review – A formal examination of a project conducted by an organization other than the development organization.

Independent Verification and Validation (IV&V) – A process whereby the products of the software development life cycle phases are independently reviewed, verified, and validated for completeness and accuracy.

Indicator – A measure or combination of measures that provides insight into a program issue or concept.

Indicators of Attack (IOA) – Indicators of attack (IOA) are similar to indicators of compromise (IOCs), but rather than focusing on forensic analysis of a compromise that has already taken place, indicators of attack focus on identifying attacker activity *while* an attack is in process.

Indicators of Compromise (IOC) – Indicators of compromise (IOCs) are pieces of digital data, such as that found in system log entries or files, that identify potentially malicious activity on a system or network.

Information – Data and records. The North Carolina Public Records Law defines public records as "all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions." N.C.G.S 132-1.

Information Assets – Information relevant to an enterprise's business function, including captured and tacit knowledge of employees, customers or business partners; data and information stored in highly-structured databases, or in textual form and in less-structured databases such as messages, e-mail, workflow content and spreadsheets; information stored in digital and paper documents; purchased content; and public content from the Internet or other sources.

Information Distribution – Making needed information available to project stakeholders on a timely basis.

Information Processing Resources – Electronic computing and communications hardware, software, networks, and information.

Information System – An information system is composed of a collection of hardware, software, information and the interconnections, including wireless technology, between these components.

Information Technology (IT) – The electronic data processing of goods and services as well as telecommunications goods and services, microprocessors, software, information processing, office systems, any services related to the foregoing, and consulting or other services for the design or redesign of information technology supporting business processes.

Equipment, telecommunications, video telecommunications, software, and purchased services such as any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The term electronic and information technology includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not information technology.

Information Technology Security Event – *See*, Cybersecurity Incident.

Information Technology Security Records – Public records, as defined by law, that describe security features of electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems, including hardware or software security, passwords, or security standards, procedures, processes, configurations, software, and codes.

Infrastructure – The physical hardware and environments used to interconnect computers and users that include the transmission media, such as telephone lines, wide and local area network cables, satellites and antennas, routers, repeaters, and other devices that control transmission paths. Infrastructure also includes the software used to send, receive, and manage the signals that are transmitted. Examples of infrastructure include computer operating systems (e.g., z/OS, Windows, Unix), database software, networks, TCP/IP and cyber security.

Infrastructure-as-a-Service (IaaS) – A model of service delivery whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service

upon which a platform to develop and execute applications can be established. Security provisions beyond the basic infrastructure are carried out mainly by the State agency.

Initiation – Organization commitment to a project or phase of a project (Project Initiation).

Input – Data from an external source.

Inspection – A semiformal to formal evaluation technique in which a software product is examined by a person or group other than the originator to detect faults errors and violations of development standards. Sometimes called a walkthrough.

Instant Messaging (IM) – A broad range of technologies that allow individuals to digitally communicate in real time over a LAN or the Internet. These technologies can require the installation of client software or they can be web based. IM conversations can occur PC-to-PC, phone-to-phone, PC-to-phone and phone-to-PC.

Integration – Describes the work, or device, required to connect two different systems that were not originally designed to work together. It could also be a process in which separately produced components or subsystems are combined, and problems in their interactions are addressed.

Integration Test – Testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them.

Integrity – The need to ensure that information has not been changed accidentally or deliberately and that it is accurate and complete.

Integrity Check – A process used to validate current configuration settings to ensure only authorized modifications have been made.

Interactive – A process where a request is processed immediately and a response is received.

Inter-Agency Wide Area Network (WAN) – A privately routed Wide Area Network (WAN) which includes RFC 1918 address definitions and allows private to private (without NAT) network access between agencies. While each agency is responsible for determining access in and out of their respective agency's firewall, the Inter-Agency WAN is considered to be a public network since traffic traverses public network circuits.

Interface – The point of information, or requested information exchange from an individual and application. Also, a connection between two devices or systems.

Internal Access Control – Protects information that is under the management of the enterprise.

Internal Interface – The point where the software system under development interacts with other components of the system under development.

Internet – The global collection of networks that communicate with each other using the Internet Protocol.

Internet of Things (IoT) – The IoT is a network of devices that are embedded with electronics, software, sensors, and network connectivity, which enable these devices to collect and exchange data. The IoT links devices to the Internet and allows them to be sensed and controlled remotely across existing network infrastructure. The IoT includes such devices as mobile computing devices, smart thermostat systems, refrigerators, washer/dryers, heart monitoring implants, automobiles with built-in sensors, and key fobs.

Internet Control Message Protocol (ICMP) – An Internet standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Key Exchange (IKE) – Provides secure management and exchange of cryptographic keys between distant devices.

Internet Protocol (IP) – A networking protocol used to communicate between computers on networks. IP is the basic protocol of the global Internet.

Internet Protocol Security (IPSec) – A security protocol defined for IP networks that operates at the network layer in TCP/IP communications protocols. IPSec adds header extensions to the IP communications protocol and is designed to provide end-to-end security for packets traveling over the Internet. IPSec defines two forms:

1. **Authentication Header (AH)** – Sender authentication and integrity, but not confidentiality.

2. **Encapsulation Security Payload (ESP)** – Sender authentication, integrity, and confidentiality.

A framework for a set of protocols for security at the network or packet processing layer of network communication.

IP Address – A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Forwarding – IP forwarding is an operating system option that allows a host to act as a router. A system that has more than one network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP Source Routing – A mechanism that allows a system to specify the routes a piece of network traffic will employ while traveling from the source system to the destination system.

IP Spoofing – The technique of supplying a false IP address.

Interoperability – "Interoperability" has two meanings: (1) The ability of systems, personnel, or organizations to provide services to and accept services from other systems, personnel, or organizations, and to use the services so exchanged so that these organizations can operate together effectively; (2) A condition that is realized among electronic communications operating systems or grids and/or among individual electronic communications devices, when those systems and/or devices allow the direct, seamless, and satisfactory exchange of information and services between the users of those systems and devices. (FEMA)

Interoperable Communications – Communications that provide the capability to perform Essential Functions, in conjunction with other organizations, under all conditions. (FEMA)

Intranet – Intranet is defined as any device designated as a private network behind a firewall that is implemented according to the security requirements of the Statewide Information Security Manual. It includes applications and network resources that are accessed only by internal users on the trusted network, as contrasted with public Internet users.

Intrusion Detection System (IDS) – Software that detects unauthorized access or misuse of a computer system. A security management system for computers and networks. An IDS 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 organization) and misuse (attacks from within the organization).

1. **Host** – Host-based intrusion detection systems use information from the operating system audit records to watch all operations occurring on the host upon which intrusion detection software has been installed. These operations are then compared with a pre-defined security policy. The analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilized by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

2. **Network** – A network-based IDS system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment. Network traffic on other segments, and traffic on other means of communication (like phone lines) can't be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment to which it is attached. Packets are considered to be of interest if they match a signature. Network-based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks, which may be missed by host-based intrusion detection mechanisms.

IDS systems are based on one of the following detection schemes:

1. **Anomaly Detection Model** – The IDS detects intrusions by looking for activity that is different from a user's or system's normal behavior.

2. **Misuse Detection Model** – The IDS detects intrusions by looking for characteristic patterns or signatures of known attacks.

Intrusion Prevention System (IPS) – Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security devices that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about those incidents, attempt to block/stop activity, and report activity. In addition, IPSs may be used to identify problems with security policies, document existing threats, and deter individuals from violating security policies. IPSs use several response techniques, which involve the device stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content. The types of IPS technologies are distinguished primarily by the types of events they monitor and the ways in which they are deployed. The following are the types of IPS devices:

1. **Network-Based** – IPS which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.

2. **Network Behavior Analysis (NBA)** – which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems).

3. **Host-Based** – which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

Investment Cost – The total of project cost (Initiation through Closeout phases) plus five (5) years of Operations and Maintenance costs.

Investor Maps – Multi-dimensional graph-views that enable an agency to effectively manage its technology investment portfolio and draw attention to areas of risk and visually portray the technology investment strategy. For example, dimensions like ROI, time to return, degree of fit with business objectives, budget, performance and risk can all be used to analyze the distribution of technology spending.

Invitation for Bid (IFB) – Equivalent to a request for proposal (RFP) in a narrow view. (PMI)

Iterative Development – The repetition of a set of development phases in short successive combinations.

J

K

Kill Chain – The Cyber Kill Chain is a model for identification and prevention of cyber intrusion activity. The model identifies what cyber adversaries must complete to achieve their objective. The kills chain involves several threat stages that are as follows:

- Reconnaissance: Intruder selects a target, researches it, and attempts to identify vulnerabilities in the target network.
- Weaponization: Intruder creates a remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
- Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives).
- Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
- Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
- Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.
- Actions on Objective: Intruder takes action to achieve his/her goals, such as data exfiltration, data destruction, or encryption for ransom.

The actions to take to defend against the cyber kill chain are as follows:

- Detect: determine whether an attacker is poking around
- Deny: prevent information disclosure and unauthorized access
- Disrupt: stop or change outbound traffic (to attacker)
- Degrade: counter-attack command and control
- Deceive: interfere with command and control
- Contain: network segmentation changes

L

L2TP - Layer 2 Tunneling Protocol

LAN – Local Area Network

LATA – Local Access and Transport Area

LDAP – Lightweight Directory Access Protocol

Lag – The amount of time after one task is started or finished before the next task may be started or finished.

Language – A means of communication, with syntax and semantics, consisting of a set of representations, conventions, and associated rules. (IEEE)

Laptop – A portable personal computer with a clamshell form factor suitable for mobile use. A laptop combines the components and inputs of a desktop computer, including display, speakers, keyboard and pointing device (such as a touchpad or a trackpad) into a single device.

Lattice Based Access Control – A variation of Mandatory Access Control and Non-Discretionary Access Control. This model allows both upper and lower limits of access capabilities for every subject and object (directory or file) relationship. Information flow is concerned with flow from one security class (also called security label) to another. These controls are applied to objects and the operation requested.

Layer 2 Tunneling Protocol (L2TP) – A tunneling protocol, which allows IP and non-IP traffic to be transported across many different types of networking medium.

Least Privilege – The principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

Legacy System – In-place systems using older technologies.

Lessons Learned – Information (positive or negative) resulting from feedback on project performance that may benefit future projects.

Life Cycle – A period of time that starts when a software product is conceived (concept formation) and ends when the software is no longer available for use (retirement). It also means a collection of phases that indicate / monitor an application's maturity.

Life Cycle Costing – The concept of including acquisition, operating, and disposal costs when evaluating various alternatives.

Lightweight Directory Access Protocol (LDAP) – A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Limited Production – A production system that is rolled out to a predetermined subset of users and proven to perform as expected.

Listing – An orderly display or printout of data items. (IEEE)

Liteware – A term for software that is distributed freely in a version having less capability than the full commercial version. Liteware is designed to provide a potential customer with a sample of the "look-and-feel" of a product and a subset of its full capability.

Local Access and Transport Area (LATA) – One of 196 local geographic areas within the United States within which a local telephone company may offer telecommunications services - local or long distance.

Local Area Network (LAN) – A short distance data communications network used to link computers and peripheral devices (such as printers, scanners, IP phones) under some form of standard control. A LAN can be extended with point-to-point wireless access points, thereby extending the coverage area inside large buildings or to nearby buildings within the campus.

Lockout – A computer resource allocation technique in which shared resources are protected by permitting access by only one device at a time. (IEEE)

Loosely Coupled – An approach to application development where application logic is implemented as distinct executable modules or separate services and components. If changes occur, it is easy to deploy the change since it does not affect other application components.

M

MAC – Mandatory Access Control or Media Access Control

MAN – Metropolitan Area Network

MAO – Maximum Acceptable Outage

MDM – Mobile Device Management

MFA – Multi-Factor Authentication

MOM – Message-Oriented Middleware

MS-ISAC – Multi-State Information Sharing & Analysis Center

MTBF – Mean Time Between Failures

MTA – Maximum Time in Alternative Operations

MTD – Maximum Tolerable Downtime

MTTR – Mean Time To Repair

Maintainability – The ease with which maintenance support and changes can be performed on a computer system.

Maintenance – Ongoing activity that keeps software functioning in a technical and business environment (production). Maintenance may be corrective maintenance (defect repair), adaptive maintenance (preventing a defect before it occurs in a changed environment), or perfective maintenance (modifications to support business functional requirements).

Malware – (malicious software): Any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

Mandatory Access Control (MAC) – Access control that is used in military and highly sensitive information systems and networks. A MAC policy dictates whether an operation should be permitted or denied and does not allow a user to override the control.

Master Schedule – An executive summary that identifies the major components of a project against which dates for achievement are estimated, particularly those achievement dates designated as milestones.

Maturity Review – A plan for periodically reviewing the effectiveness of the Statewide Architecture Framework to establish point-in-time conditions from which action plans will be developed.

Maximum Acceptable Outage (MAO) – This is the timeframe during which a recovery must become effective before an outage compromises the ability of an organization to achieve its business objectives and or survival. (FEMA) *See*, MTD; MTA.

Maximum Time in Alternative Operations (MTA) – *See*, Maximum Acceptable Outage (MAO)

Maximum Tolerable Downtime (MTD) – The maximum number of hours for which it is acceptable that a function can be interrupted following a continuity event. (FEMA) *See*, Recovery Time Objective; Maximum Acceptable Outage.

Mean Time To Failure (MTTF) – The length of time a device or other product is expected to last in operation. MTTF is one of many ways to evaluate the reliability of pieces of hardware or other technology.

Mean Time To Repair (MTTR) – The average time that it takes to perform corrective actions on a device to restore its functionality.

Measure – 1) To estimate or appraise by a criterion. 2) The result of counting or otherwise quantifying an attribute of a process or product. Measures are numerical values assigned to software attributes according to defined criteria. Often the terms measure and metric are used synonymously.

Measurement – The act or process of measuring. This process can be based on estimation or direct measurement.

Media Access Control (MAC) Address – The hardware address that uniquely identifies each node of a network.

Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) – Written agreements between organizations that require specific goods or services to be furnished or tasks to be accomplished by one organization in support of the other. (FEMA)

Mesh Networking – A way to route data between nodes employing one of two connection arrangements: *full mesh* topology or *partial mesh* topology. In the *full mesh* topology, each node is connected directly to each of the others. In the *partial mesh* topology, some nodes are connected to all the others, but some are connected only to those other nodes with which they exchange the most data. One advantage of a mesh network is that it offers redundancy. If one node can no longer operate, the rest can still communicate with each other, directly or through one or more intermediate nodes.

Message Digest – A summary of a message that can act as a "fingerprint" for the message and can be used to vouch for the integrity of a message. Message digests are used to ensure the *integrity* of information by allowing a recipient to detect any change to the original content of a message. The message content is processed by a mathematical 'hash' function to produce a small numeric value called a *message digest*. Hash functions are mathematical algorithms specially designed to produce unique numeric values based on the exact content of the message - even the slightest change to a message content, such as adding or deleting a comma, would produce a *different* message digest. To verify information has not been modified, a recipient applies the same hash function on a message to generate a second message digest. If the resulting message digest matches the original message digest, the information has not been changed.

Message-Oriented Middleware (MOM) – Middleware that delivers messages from one software module to another. Modules do not have to execute on the same machine. Analogous to the US Mail. The mail is typically delivered when you are at work; you pick it up at your convenience.

Metric – Quantitative measures of extent or degree to which software possesses and exhibits a certain characteristic, quality, property, or attribute.

Metropolitan Area Network (MAN) – A high speed intra city network that links multiple locations within a campus, city or LATA.

Milestone – A significant point or event in the project. (PMI)

Milestone Schedule – A summary-level schedule that identifies the major schedule milestones. (PMI)

Mission Essential Functions (MEFs) – The limited set of organization-level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities. (FEMA)

Mitigation – Taking steps to lessen risk by lowering the probability of occurrence or the impact of occurrence.

Mobile Code – Software that is transferred between systems and executed on a local system without explicit installation or execution by the recipient. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript, which are common installations on most end user workstations. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., tablet computers and smartphones). Active X and Java are examples of mobile code that can inadvertently breach agency network defenses.

Mobile Computing Device – A portable computing device that (1) has a small form factor such that it can easily be carried by a single individual; (2) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (3) possesses local, non-removable or removable data storage; and (4) includes a self-contained power source. Mobile computing devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include laptop computers, smart phones, tablets, and e-readers.

Mobile Device Management (MDM) – The administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within State government, while simultaneously protecting the State Network.

Model – A way of looking at reality, usually for the purpose of abstracting and simplifying it to make it understandable in a particular context.

Modular Programming – Programming that has as its fundamental assumption that a large piece of software should be separated into its constituent parts or modules thereby making for easier and faster development and maintainability. Modules were traditionally called subroutines or functions and now are often called objects.

Modularization – The splitting up of a software system into a number of manageable phases.

Monitoring – The gathering of information through software programs that track users' activities. Examples include the logging of visitors to a site by IP address, such as aol.com and ncmail.net. For site security and to ensure that a service remains available to all users, electronic monitoring can employ software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage to an information technology system. The programs often create summary statistics, which are used for such

purposes as assessing the number of visitors to the different section of an Internet site, the information that is of most and least interest, and identifying system performance or problem areas.

Monitoring also includes the gathering of information on individuals' specific use of information technology.

Monolithic – A computer program in which all instructions are combined into a single large software module. Monolithic programs are inflexible and are difficult to modify to support changing business requirements.

Multi-Factor Authentication (MFA) – A type of authentication that requires more than one method or factor to be used. The three common types of authentication methods include something you know (e.g. a password, passphrase, or PIN), something you have (e.g. an ID badge or a cryptographic key), and something you are (e.g. a fingerprint or other biometric data). Multi-factor authentication refers to the use of more than one of these factors. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

Multi-State Information Sharing & Analysis Center (MS-ISAC) – The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for U.S. State, Local, Territorial, and Tribal (SLTT) governments. It collects, analyzes and disseminates actionable threat information to its members and provides members with tools to mitigate risks and enhance resiliency.

Multi-Year Strategy and Program Management Plan (MYSPMP) – A plan that guides the development of the Continuity program over a set number of years via process that ensures the maintenance and continued viability of Continuity plans. (FEMA)

N

NAT – Network Address Translation

NCSR – Nationwide Cybersecurity Review

NIST – National Institute of Standards and Technology

Nation State – A nation state threat actor is a type of Advanced Persistent Threat (APT). The nation state threat actor receives direction and support from an established nation state (government). The line between nation-state cyber activity and cybercrime is often blurred as organized crime groups are afforded a degree of support.

National Continuity Coordinator (NCC) – The Assistant to the President for Homeland Security and Counterterrorism is the NCC. The NCC is responsible for coordinating, without

exercising directive authority, the development and implementation of Continuity policy for executive branch organizations. (FEMA)

National Continuity Policy – It is the policy of the United States to maintain a comprehensive and effective Continuity capability composed of COOP and COG programs in order to ensure the preservation of our form of Government under the Constitution and the continuing performance of National Essential Functions under all conditions (NSPD 51/HSPD 20, National Continuity Policy). (FEMA)

National Essential Functions (NEFs) – The eight functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities. (FEMA)

National Institute of Standards and Technology (NIST) – Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. The NIST mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade and improve the quality of life. The organization publishes computer security standards and guidelines on the Computer Security Resource Center web site at https://csrc.nist.gov.

Nationwide Cybersecurity Review (NCSR) – A free, anonymous, annual self-assessment survey that is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing & Analysis Center (MS-ISAC).

Need-to-Know – Access to confidential records only when such access is necessary in the performance of tasks or services essential to the fulfillment of a work assignment, contract or program.

Netmask – A 32-bit number indicating the range of IP addresses residing on a single IP network, subnet, or supernet. The number can be represented in hexadecimal or numerical format.

Network – A series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks. It is also the physical hardware and software connections between computers that allow information to be shared and electronic communication to take place. A network printer, for example, allows many PCs to print to it, even though the PCs are not hardwired directly to the printer. The term network includes LAN, WAN, MAN and Campus.

Network Address Translation (NAT) – The translation of an Internet Protocol address used within one network to a different IP address known within another network. Commonly used to convert between public IP addresses and private IP addresses at the connection between the public Internet and a private network.

Network Analysis – The process of identifying early and late start and finish dates for the uncompleted portions of project activities.

Network Based Intrusion Detection – *See,* Intrusion Detection

Network Diagram – The logical representation of tasks that defines the sequence of work in a project.

Network Domain – *See,* Statewide Architecture Framework.

Network Zone – Any area within an organization's network that is separated from another by logical or physical access controls, such as a firewall. The purpose of network zones is to segregate different network resources based upon access restrictions. For instance, database servers would be installed in a database secure zone separate from the application server zone and the web server zone.

N-tier – A method of application development where application logic is divided into tiers. Business rules are implemented as distinct executable modules and are loosely coupled and separate from other business rules, the code that implements the user interface, and the code that provides data access. N-tier programming provides many benefits including ease of maintenance, increased security and flexibility in platform deployment.

NIST Vulnerability Database – A free resource which to date contains more than 5,268 known vulnerabilities. The tool is located at https://nvd.nist.gov/.

Nonconformance – A deviation from specified standards, procedures, plans, requirements, or design.

Non-Critical – In the agency's opinion, the loss of an application will have little or no impact to Statewide and/or agency core functions, processes and activities or the core functions, processes and activities associated with a program within the agency.

Non-Developmental Software (NDS) – Deliverable software that is not developed under contract but is provided by the vendor, contractor, or third-party supplier.

Non-Repudiation – Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

O

OOP – Object Oriented Programming

OSI – Open Systems Interconnection

Object – An entity that contains or receives data.

Object Oriented Programming (OOP) – A programming technique that focuses on the idea of defined data structures, with a controlled means of accessing and modifying them. These structures are presented to the user as objects (a set of data defined in a specific way). The user

manipulates the object and the object in turn manipulates the data. OOP differs from procedural programming by providing a number of key features such as encapsulation (hiding information within a structure), abstraction (grouping details into a single common concept), inheritance (ability to derive attributes and methods contained in a previously defined object), and polymorphism (one name, many forms).

Objective – A concise statement of what a project is to achieve. The objectives are subordinate to higher level goals.

Open Source – A program in which the source code is available (licensed) to the general public for use and/or modification from its original design free of charge. Open source code is typically created as a collaborative effort in which programmers improve upon the code and share the changes within the community.

Open Source COTS – Software that is commercially available from the manufacturer for a fee. The fee, however, provides a financial model for future development and maintenance of the software. The fee is usually accompanied by support and maintenance agreements. The manufacturer, instead of a community of users, manages bug fixes, enhancements, quality assurance and code reviews. The community of users may contribute to the product, but the manufacturer is responsible for coordination of changes.

Open Systems Interconnection (OSI) – A standard description or reference model for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many - if not most – products involved in telecommunication attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

Operating System – Required software designed to interact with the hardware and software of a specific data-processing system in order to allow users and application programs to utilize the system.

Operations and Maintenance Cost – Cost to operate, support, and maintain a system after development. Operations and maintenance cost should be calculated on a five (5) year time line.

Operations and Maintenance Phase – The period of time in the software life cycle during which the software product is employed in its operational environment. (IEEE)

Opportunity Cost – The potential net benefit, or value, of an information technology investment that is lost by selecting an alternative investment.

Opportunistic Cyber Crime – Any criminal attack that arises from chance discovery of a loophole in the system, which permits access to unauthorized information.

Orders of Succession – Orders of succession provide for the orderly and predefined assumption of senior agency offices during an emergency in the event that any officials are unavailable to execute their legal duties. (FEMA)

Organization Head – The highest-ranking official of the organization, or a successor or designee who has been selected by that official. (FEMA)

Organizations – Those executive departments enumerated in 5 U.S.C. § 101, together with the DHS, independent establishments as defined by 5 U.S.C. § 104(1), Government corporations as defined by 5 U.S.C. § 103(1), and the United States Postal Service. The departments, agencies, commissions, bureaus, boards, and independent organizations are referred to in this document as "organizations." (FEMA)

OSI Layers – A standard description or model for how messages should be transmitted between any two points in a telecommunication network. The main idea in OSI is that the process of communication between two end points in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions. Each communicating user or program is at a computer equipped with these seven layers of function. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user or program.

The actual programming and hardware that furnishes these seven layers of function is usually a combination of the computer operating system, applications (such as your Web browser), TCP/IP or alternative transport and network protocols, and the software and hardware that enable you to put a signal on one of the lines attached to your computer. OSI divides telecommunication into seven layers. The layers are in two groups. The upper four layers are used whenever a message passes from or to a user. The lower three layers (up to the network layer) are used when any message passes through the host computer or router. Messages intended for this computer pass to the upper layers. Messages destined for some other host are not passed up to the upper layers but are forwarded to another host. The seven layers are as follows:

- **Layer 7** – The application layer...The layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is not the application itself, although some applications may perform application layer functions.)

- **Layer 6 –** The presentation layer...The layer, usually part of an operating system that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). Sometimes called the syntax layer.

- **Layer 5** – The session layer...The layer that sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It deals with session and connection coordination.

- **Layer 4 –** The transport layer...The layer that manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer.

- **Layer 3** – The network layer...The layer that handles the routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). The network layer does routing and forwarding.

- **Layer 2 –** The data-link layer...The layer that provides synchronization for the physical level and does bit-stuffing for strings of 1s in excess of 5. It furnishes transmission protocol knowledge and management.

- **Layer 1** – The physical layer...The layer that conveys the bit stream through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier.

Output – Pertaining to data transmitted to an external destination. (IEEE)

Outsource – The practice of contracting out a project, service, or information technology operation to a third party.

P

PCI – Payment Card Industry

PERT – Program Evaluation and Review Technique

PHI – Protected Health Information

PING – Packet Internet Groper

PKI – Public Key Infrastructure

POA&M – Plan of Actions and Milestones

Package Acquisition – The purchase, or lease, of software from an outside source.

Package System – A “store bought” pre-defined application solution meeting a specific business need.

Packet Internet Groper (PING) – A utility used to determine whether a particular computer is currently connected to the Internet. It works by sending a packet to the specified IP address and waiting for a reply.

Padding – A standard project management tactic used to add extra time or money to estimates to cover for the uncertainty and risk of predicting future project activities.

Partition – To segment or to separate into components. Servers can be partitioned according to the function they provide, the resource they control, or the database they own.

Password – The secret code used to access a computer, computer system or computer network.

Password Authentication – Access to an information system is authenticated with a password that follows the security standard set forth in the Statewide Information Security Manual. All passwords shall be encrypted in storage and in transit where supported by the application and/or system.

Patch – A repair job for a piece of programming software. Patches are usually released for three reasons:

1. To fix faults in an application or operating system.
2. To alter functionality or to address a new security threat.
3. To change or modify software configuration to make it less susceptible to attacks and more secure.

Parallel Testing – The task of executing both the "new" and the "old" systems and comparing results.

Pareto Diagram – A histogram, ordered by frequency of occurrence, which shows how many results were generated by each individual cause.

Path – A sequence of lines and nodes in a project network.

Path Testing – Testing to ensure that all logic paths within the code are exercised (Branch Testing).

Payback – A measure of time that indicates how much time will be required to recover (payback) an original investment.

Payment Card Industry (PCI) Data – PCI data is any cardholder data and authentication data. The primary account number (PAN) is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected

in accordance with applicable PCI Data Security Standard (DSS) requirements. Cardholder data and Authentication data may include the following elements:

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code
- Full track data (magnetic-stripe data or equivalent on a chip)
- CAV2/CVC2/CVV2/CID
- PINs/PIN blocks

Peer-to-Peer – A communications model in which each party has the same capabilities and either party can initiate a communication session. In recent usage, peer-to-peer has come to describe applications in which users can use the Internet to exchange files with each other directly or through a mediating server.

Peer Review – A technical review in which a project artifact is inspected by a small group of experts.

Perfective Maintenance – Software maintenance performed to improve the performance, maintainability, or other attributes of a computer program. (IEEE)

Performance – The calculation of achievement used to measure and manage project deliverables.

Performance Evaluation – The technical assessment of a system or process to determine how effectively operating objectives have been achieved.

Performance Requirement – A requirement that imposes conditions on a functional requirement (e.g., speed, accuracy, storage usage). (IEEE)

Performance Testing – Verification of batch and on-line response time through volume and stress testing to determine throughput, response time, and availability.

Personal Computing Device – *See*, Mobile Computing Device.

Personal Firewalls – Firewalls that are installed and run on individual desktops or laptop computers.

Personal Information or Personally Identifiable Information (PII) – Under state law, personal information is a person's first name or first initial and last name in combination with other identifying information (*See*, N.C.G.S. 75-61(10)). Identifying information is defined by state law as:

a. Social security or employer taxpayer identification numbers.
b. Driver's license, state identification card, or passport numbers.

c. Checking account numbers.
d. Savings account numbers.
e. Credit card numbers.
f. Debit card numbers.
g. Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
h. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
i. Digital signatures.
j. Any other numbers or information that can be used to access a person's financial resources.
k. Biometric data.
l. Fingerprints.
m. Passwords.
n. Parent's legal surname prior to marriage. (N.C.G.S. 14-113.20(b), N.C.G.S. 132-1.10)
o. Federal law also restricts the use of personal information by state motor vehicle agencies. (18 U.S.C. 2721 – Driver's Privacy Protection Act)

Personally-Owned Device – A device that is owned by an individual.

Pharming – The practice of redirecting computer users from legitimate websites to fraudulent ones for the purposes of extracting confidential data.

Phase – The divisions of a software development life cycle into discrete stages (e.g., requirements, design, code, test, etc.). The period of time during the life cycle of a project in which a related set of software engineering activities is performed.

Phase Transition Review – Review at the end of a life cycle phase.

Phishing – A form of fraud in which an attacker masquerades as a reputable entity or person in in an electronic communication, such as email. The attacker may use phishing emails to distribute malicious links or attachments to their victims that can perform a variety of functions, including the extraction of login credentials or account information, or other sensitive information.

Pilot – An approach designed to evaluate a preliminary version of a system in a simulated production environment.

Pilot Testing – The testing process, equivalent to beta testing, that organizations use to test applications in a pre-production environment.

Plan of Actions and Milestones (POA&M) – A POA&M is a plan that describes specific measures to be taken to correct deficiencies in an information system that were found during a security assessment. A POA&M will assist organizations in identifying, assessing, prioritizing, and monitoring the progress of corrective measures for security weaknesses that were identified in systems. A POAM should identify the tasks needed to correct the deficiency, the resources

required to make the plan work, milestones in completing the tasks, and scheduled completion dates for the milestones.

Planned Finish Date – A point in time when work is scheduled to end for the task or activity.

Planned Start Date – A point in time when work is scheduled to begin on the task or activity.

Platform – The hardware and support software with which a program is intended to operate.

Platform-as-a-Service (PaaS) – A model of service delivery where the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. Security provisions are split between the provider and the State Agency.

Platform Domain – *See*, Statewide Architecture Framework.

Policy – Statement of intent by a governing body.

Port – On computer and telecommunication devices, a port is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Various common Internet protocols communicate on specific ports. The Web uses port 80, FTP uses ports 20 and 21, and Telnet uses port 23.

Portable Computing Device – *See*, Mobile Computing Device.

Portable Storage Device – *See*, Removable Media.

Portfolio – A collection of related items that are grouped for ease of management and the viewing of performance of applications.

Portfolio Management – The centralized management of one or more portfolios, which includes identifying, prioritizing, authorizing, managing, and controlling projects, programs, and other related work, to achieve specific strategic business objectives. (PMI)

Postcardware – Freeware that requires the user to send the software provider a postcard as the form of payment.

Preliminary Design Review – Phase transition review for the preliminary high-level (architectural) design life cycle phase. Also known as Architectural Design Review.

Pre-Shared Key – A TKIP or CCMP passphrase used to protect your network traffic in WPA and WPA2. Some manufacturers use the term “pre-shared secret” instead.

Primary Mission Essential Functions (PMEFs) – Those organization MEFs, validated by the NCC, which must be performed in order to support the performance of NEFs before, during, and in the aftermath of an emergency. PMEFs need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed. (FEMA)

Primary Operating facility – The facility where an organization's leadership and staff operate on a day-to-day basis. (FEMA)

Primary Server – An authoritative server for which the DNS zone information is locally configured. This is sometimes known as a Master Server.

Principles – *See,* Architectural Principles.

Private Addressing – The Internet Assigned Numbers Authority (IANA) has set aside three IP address ranges for use by private or non-Internet connected networks. This is referred to as Private Address Space and is defined in Request for Comments (RFC) 1918. The reserved address blocks are: 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255 (172.16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix).

Private Network – A network that uses private Internet Protocol (IP) address space, following the standards set by RFC 1918 and RFC 4193. These addresses are commonly used for home, office, and enterprise local area networks (LANs), when globally routable addresses are not mandatory, or are not available for the intended network applications. Private network IP addresses are not allocated to any specific organization, and IP packets addressed by them cannot be transmitted onto the public Internet. Anyone may use these addresses without approval from a regional Internet registry. If a private network needs to connect to the Internet, it must use either a network address translator (NAT) gateway, or a proxy server that utilizes a public network address.

Privileged Account – An account of an information system that has more authority and access than a normal user account. Examples of privileged accounts include those that have root access, system administrator access, and accounts associated with database ownership and router access.

Problem – In risk management, a problem is a risk that has materialized. Deviation from the normal or expected results.

Problem Resolution – The finding of a solution to technical, scheduling, or resource availability problems.

Procedure – A prescribed method, or technique, for performing work.

Process – The step-by-step sequence of activities (systematic approach) that must be carried out to complete a project. It is also a collection of related, structured activities or chain of events that produces a specific or defined output or result.

Process Automation Application – Specific programs that manage equipment (e.g., Printer Control Language).

Process Model – A model of a software project that depicts the relationship of the project functions, activities, and tasks to the major milestones, baselines, reviews, work products, project deliverables, and formal approvals that span the project.

Procurement Plan – A formal, documented, and approved plan to procure needed resources (hardware, software, or networks) and staff needed to complete a project.

Product – The end result of a process.

Product Baseline – The initial approved technical documentation defining a configuration item. (IEEE)

Product Integration – Assembling individual hardware and software components into a functional whole.

Production Library – A software library containing software approved for current operational use. (IEEE)

Program – A specific set of ordered operations for a computing device to perform.

Program Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to the core functions, processes and/or activities associated with a program within this agency.

Program Evaluation and Review Technique (PERT) – A method that uses the concepts of milestones, activities, and slack time to calculate the critical path. The chart, which resembles a flow chart, depicts a box to represent each project task and a line connecting two boxes to represent the relationship between tasks.

Programming – The art of writing, in a computer understandable language, a set of instructions that produces software.

Programming Language – An artificial language used to write instructions that can be translated into machine language and then executed by a computer.

Project – A temporary endeavor (begin and end dates) undertaken (resources and plan) to create a unique product or service (business functional requirement). The combined resources (people,

machines, materials), processes, and activities that are dedicated to building and delivering a product, or service to a customer.

Project Cost – The cost of project development cost from Project Initiation through Project Closeout phases.

Project File – A central repository of material pertaining to a project. (Project Notebook) (IEEE)

Project Duration – The time it takes to complete the entire project.

Project Lifecycle – A collection of generally sequential project phases whose name and number are determined by the control needs of the organization involved in a project.

Project Management – The combination of systems, techniques, and people required to successfully complete a project on time and within budget. (PMI)

Project Manager – The senior person responsible for an entire project.

Project Plan – A formal, approved document that describes the technical and management approach to be followed for a project and that is used to guide both project execution and project control.

Project Sponsor – The department customer who will authorize project initiation, and who will receive, accept, and use the software product or service.

Promiscuous Mode – When a network interface card (NIC) is set to read all network packets regardless of their address. This is a mode used by network administrators to diagnose network problems but also by unauthorized persons trying to eavesdrop on network traffic (which might contain passwords or other information). Network IDS sensors often use promiscuous mode to observe traffic "passing by" the sensor.

Proof of Concept – Software written to gather requirements, prove or test a technology, language, environment, or approach. A proof of concept should not be implemented as a production system.

Proprietary – A privately owned and controlled specification. A proprietary architecture is one that is owned by a company or institution. This is not consistent with the Statewide Architecture Framework and with accepted industry practice.

Protected Health Information (PHI) – PHI is defined in federal law (45 CFR 160.103) and pertains to information that contains the following types of data:

- Individually identifiable health information
- Transmitted or maintained in any form or medium by a Covered Entity or its Business Associate

- Health information including demographic information;
- Relates to an individual's physical or mental health or the provisions of or payment of health care
- Identifies the individual

Protocol – A standardized, formal description of message formats and the associated rules two computers must follow to exchange those messages. Protocols allow data to be taken apart for faster transmission, to be transmitted, and then to be reassembled at the destination in the correct order. The protocol used determines the way errors are checked, the type of compression, the way the sender indicates the end of the transmission, and the way the receiver indicates that the message has been received. Protocols can describe low-level details of machine-to-machine interfaces (*e.g.*, the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (*e.g.*, the way in which two programs transfer a file across the Internet).

Prototype – A small working version of a proposed system used to gather requirements, validate requirements, "show" what the system will look like, or demonstrate proof-of-concept.

Proxy Server – A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with, or part of, a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Pseudo Code – A combination of programming language and natural language used for computer program design.

Public Access – Anonymous access to applications that do not require authentication, such as access to web pages**.**

Public Agency – Any North Carolina governmental agency including North Carolina state government, county and city political subdivisions of North Carolina, primary, secondary, vocational technical and higher education institutions within North Carolina entitled to services provided by the North Carolina Department of Information Technology (DIT).

Public Domain – Programs that are not copyrighted because their authors intended to openly share them. Programs in the public domain can be used without restriction as components of other programs. It is important to understand the history of public domain software to ensure the entire source code is in the public domain. Where some components may not be in the public domain, the entire source may be subject to a more restrictive license agreement.

Public Key – The publicly disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key / Private Key Cryptography – A cryptography technique that gives a user a 'public key' for others to communicate with the user and a 'private' key which is used as a digital signature. Also referred to as "asymmetric key cryptography" because different keys are used to encrypt and decrypt.

Public Key Certificate – An electronic document that contains a user's public key.

Public Key Infrastructure (PKI) – A PKI enables users of a public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. It includes the functions required to issue and manage the public key certificates needed for authentication. A Public Key Infrastructure consists of all the supporting services required to issue and manage digital certificates.

Public Network – A network established and operated by a telecommunications administration, or a recognized private operating agency, for the specific purpose of providing data transmission services for the public. Public networks typically use Internet Protocol (IP) addresses that are globally routed throughout the Internet. For the purpose of the Statewide Information Security Manual, public networks are deemed less secure than private networks and therefore require encryption for the transmission of confidential data.

Public Records – All documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.

Q

Quality (Product) – Conformance to business functional requirements with defect-free products. Quality reflects both the completeness of software or system features and functions, and error-free operation.

Quality (Process) – Verification and validation to established policies, standards, procedures and guidelines for software development.

Quality Assurance – Within the State of North Carolina, the process tracking and oversight function for monitoring project performance, adherence to commitments, and budget requirements.

Quality Assurance Plan – A plan that defines the activities performed to provide assurance that the software-related items delivered to the customer conform to the established and contracted

technical requirements. The Software Quality Assurance Plan also describes how the project will be audited to ensure that the policies, standards, practices, procedures, and processes applicable to the project are followed.

Quality Engineering – The process of incorporating reliability, maintainability, and other quality factors into software products.

Quality Metric – A quantitative measure of the degree to which an item possesses a given quality attribute.

R

RACF – Resource Access Control Facility

RAD – Rapid Application Development

RAID – Redundant Array of Independent Disks

RBAC – Role Based Access Control

RFP – Request for Proposal

RMF – Risk Management Framework

Ransomware – A type of malicious software (malware) that threatens to publish the victim's data or prevents users from accessing their system or personal files unless a ransom is paid. Ransomware typically encrypts the victim's data and withholds the decryption key until the ransom is paid. Sometimes, the criminal does not provide the decryption key even if the ransom is paid; therefore, law enforcement agencies state that it is best practice to not pay the ransom.

Rapid Application Development (RAD) – Methodology that emphasizes application development as an iterative prototype-to-production process.

Readiness Reporting System (RRS) – A DHS program to collect and manage Continuity capability data and assessments of executive branch organizations and their status to perform their PMEFs in support of the NEFs. The RRS will be used to conduct assessments and track capabilities at all times under all conditions, to include natural disasters, manmade incidents, terrorism, and war. (FEMA)

Reconciliation – The act of identifying and removing inconsistencies.

Reconnaissance – Gathering information on a target before the actual attack starts. Active reconnaissance is an attack in which an adversary engages a targeted network or system to gain

information about vulnerabilities. Passive reconnaissance is an attempt to gain information about targeted computer systems and networks without actively engaging with those systems.

Record – A set of data treated as a unit.

Recovery – The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following an interruption or disaster. (FEMA)

Recovery Point Objective (RPO) – The point in time to which systems and data must be recovered following an adverse event, *e.g.* the last completed transaction or the point immediately before the last backup commences. Also known as the Critical Data Point.

Recovery Time Actual (RTA) – The time frame that technology and application support staff actually takes to deliver the recovered service/application to the business. The RTA is usually determined during recovery exercises.

Recovery Time Objective (RTO) – The duration of time and a service level within which systems, applications, or functions must be restored after an outage to the predetermined Recovery Point Objective (RPO), for example, one business day.

Redundancy – The state of having duplicate capabilities, such as systems, equipment, or resources. (FEMA)

Redundant Array of Independent Disks (RAID) – A data storage technology that combines multiple physical disk drive components into one or more logical units for the purposes of fault tolerance, data redundancy, and/or performance improvement.

Re-engineering – Examination and alteration of an application system to reconstitute it in a new form (renovation). The practice of adapting existing systems to perform new or enhanced functions usually significantly different than the existing system.

Regression Test – The selective re-testing to detect errors or faults introduced during modification of a system.

Relational Database – A collection of data that is organized into tables so that relationships between and among data can be established.

Release – Specific version of a piece of software.

Release Management – The process used to manage the release of software into different environments (test, pre-production, production).

Reliability – Refers to the extent in which consistent outcomes are achieved. The degree of dependability usually expressed as the average / mean time to failure.

Registration Authority – An entity that authorizes requests for digital certificates, verifies the identity of requestors, and authorizes revocation of digital certificates. This is a component of a PKI.

Remote Access – The ability of a resource to access the state's network via an external network connection. Remote access generally occurs from remote locations such as homes, hotel rooms, and off-site offices; however, it may also occur locally within an agency's physical facilities.

1. **LAN-to-LAN connection** – A dial-up connection is used to setup a connection between two local area networks over the Internet. This arrangement is called a LAN-to-LAN connection. When a user on one network access a resource on another network, the remote access device automatically dials the nearest ISP access number to establish a connection to the appropriate remote site.

2. **Client-to-LAN connection** – The remote user dials into the nearest ISP access number to connect with the ISP's remote access server, which then forwards the traffic to central site system. This arrangement saves on long distance toll charges and eliminates the need for remote access servers at the central site.

Removable Media – Electronic storage devices that can be used to store and/or move data between computing equipment. Removable media includes electronic storage media such as compact discs, DVDs, portable USB drives, external hard drives, and flash memory cards.

Request for Proposal (RFP) – Formal statement by a department that it is soliciting enterprises to bid on a contract for a program, system or service.

Requirements – The statement of needs by a user that triggers the development of a program, system, or project. May be called business functional requirements or requirement specifications.

Requirements Allocation – The process of distributing requirements of a system to subordinate software and hardware elements.

Requirement Review – Phase transition review for the requirements life cycle phase.

Resilience – The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Examples of resilience measures include the following:

- Developing a business continuity plan
- Having a generator for back-up power
- Using building materials that are more durable

Resource Access Control Facility (RACF) – An IBM security software product that is installed on the DIT mainframe computers. Virtually everything related to accessing the DIT mainframe, including but not limited to user IDs, is stored in the RACF database.

Resource Leveling – Any form of network analysis in which scheduling decisions are driven by resource management concerns. It can also be the process of shifting resources to even out the workload of team members.

Responsibility Matrix – Chart of project roles and responsibilities.

Reuse – Hardware or software developed for one application that can be used, in whole or in part, to satisfy the requirements of another system.

Rework – Action taken to bring a nonconforming item into compliance with requirements. (PMI)

Rights and Interests Records – Records that are necessary to protect the legal and financial rights of both the Federal Government and the persons who are affected by its actions. (FEMA)

Risk – A condition or action that may adversely affect the outcome of a planned activity or the ability to deliver services.

Risk Analysis – An evaluation of the feasibility or probability that the outcome of a project will be the desired outcome.

Risk Assessment – The process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined acceptable levels of risk.

Risk Avoidance – An informed decision not to become involved in a risk situation.

Risk Management – The systematic application of management policies, procedures and practices to the tasks of identifying, assessing, treating and monitoring risk.

Risk Management Framework (RMF) – The National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle (SDLC). NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems", provides a six-step Risk Management Framework (RMF). Those steps are as follows: categorization of information systems, selection of security controls, implementation of security control, assessment of security controls, authorization of information systems, and monitoring of security controls.

Risk Management Plan – A formal documented and approved document that identifies risk, assesses the impact of the risk, and provides the project response to the risk.

Risk Management Program – Identifies and classifies risks and implements risk mitigation as appropriate. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.

Risk Mitigation – The process of removing or reducing risk. Risk mitigation may include risk analysis, or other activities designed to assess the results of risk mitigation initiatives.

Robustness – The degree to which a component can function correctly in a stressful environment. (IEEE)

Role Based Access Control (RBAC) – Also known as Non-Discretionary Access Control. A centrally administered set of controls based on the roles individuals have within an organization (e.g. bank teller, loan officer, etc.). This model simplifies management of authorization while providing an opportunity for great flexibility in specifying and enforcing enterprise-specific protection policies. This model works well for departments or organizations that have a large turnover of personnel.

Roles and Responsibilities – An explanation of the roles and responsibilities supporting the development, institutionalization, and maintenance of the North Carolina Statewide Architecture Framework to include the approval process, enforcement, custodianship, and how input from the constituency is obtained and incorporated into the body of work.

Rollout Plan – A formal, documented, and approved plan to rollout the system or product.

Root Cause – The primary cause for a problem or action.

Router – A device or, in some cases, software in a computer, that determines the next network point to which a packet of data should be forwarded toward its destination.

Rule-Based Access Control – Specific rules that indicate what can or cannot happen to an object. Routers and firewalls use this type of access control to determine which types of packets are allowed into a network and which ones are rejected. The rules are set by the administrator and cannot be modified by users.

S

SDLC – Software/System Development Life Cycle

SIEM – Security Information and Event Management

SLTT – State, Local, Territorial, and Tribal

S/MIME – Secure Multipurpose Internet Mail Extensions

SNMP – Simple Network Management Protocol

SOA – Service Oriented Architecture

SOW – Statement of Work

SSH – Secure Shell

SSID – Service Set Identifier

SSL – Secure Sockets Layer

STIG – Security Technical Implementation Guide

Scalability – The ability of a computer application or product (hardware or software) to continue to function well when it (or its context) is changed in size or volume in order to meet a user need.

Scalable – A term describing an architecture or software that can handle expansion in use as the need arises without adversely impacting systems management and operations.

Schedule – The planned dates for performing activities and the planned dates for meeting milestones.

Schedule Milestone – A significant event in the project schedule, such as an event restraining future work or marking the completion of a major deliverable. A schedule milestone has zero duration. Sometimes called a milestone activity. (PMI)

Scope – The sum of the products and services to be provided by the project.

Scope Change – Any change to the project scope. Scope changes almost always require adjustment to the project cost and schedule. ("Scope Creep" – negative control of change.)

Screen Lock – A special application that cannot be opened without a password that locks access to the computer every time a mouse and computer keyboard are idle for a specified period of time.

Screen Saver – A special application that starts every time a mouse and keyboard are idle for a specified period of time and that hides any information displayed on a computer monitor.

Secondary Server – An authoritative server that obtains information about a DNS zone from a Primary Server via a zone transfer mechanism. This is sometimes known as a Slave Server.

Secret Key Cryptography – A cryptography technique that uses a single key for both scrambling and unscrambling of data. Since only a single key is used, both parties must share this secret. Also known as symmetric key cryptography.

Secure/Multipurpose Internet Mail Extensions (S/MIME) – An application security protocol for email and store and forward messaging.

Secure Shell (SSH) – A program to securely log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

Secure Sockets Layer (SSL) – An industry standard protocol for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security – The degree to which a software product is safe from unauthorized use.

Security Audit – A periodic audit that measures whether an agency's information technology is secure and whether it conforms to established criteria.

Security Checkpoint – as related to SDLC, a review of code development at the end of each cycle of the SDLC to ensure appropriate security measures are addressed.

Security Domains – Areas within the enterprise, which adhere to a specific security policy and its enforcement. *See.* Statewide Architecture Framework.

Security Event – *See,* Cybersecurity Incident

Security Incident – *See,* Cybersecurity Incident

Security Information and Event Management (SIEM) – Technology that supports threat detection and security incident response through the real-time collection and historical analysis of security events from a variety of data sources. A SIEM also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

Security Liaison – The individual at a State agency who is assigned information technology security duties by the agency head. The liaison is appointed pursuant to G.S. § 143B-1379 and coordinates with the State CIO on information security matters.

Security Policy – A statement of intent and directive to covered agencies that specifies what they are expected to do to implement a holistic information security program.

Security Protocols – Protocols are well-defined message formats that can be applied at useful places in software or communications architectures.

Security Risk Process – The focus of security risk management is an assessment of those security risk outcomes that may jeopardize agency assets and vital business functions or services.

Security Technical Implementation Guide (STIG) – A methodology for standardized secure installation and maintenance of computer software and hardware.

Segment – A specially configured subset of a larger network. The boundaries of a network segment are established by devices capable of regulating the flow of packets into and out of the segment, including routers, switches, hubs, bridges, or multi-homed gateways (but not simple repeaters).

Separation of Duties – The use of more than one individual to handle a particular (generally important) activity.

Sequential – Pertaining to the occurrence of two or more events where one must finish before the second can begin (e.g., serial process).

Service Account – An account created by system administrators for automated use by an application, operating system, computer hardware or network device for its business purpose.

Service Broker – The North Carolina Service Broker is comprised of statewide, shared services and a supporting infrastructure. The Service Broker environment allows changes to the underlying state technical infrastructure by permitting changing the state's technical infrastructure (including middleware) with little or no modification to the supported applications. This model incorporates inter-application communication, which simplifies communication external to the application and insulates the underlying infrastructure. Source code does not have to change in response to changes in services or infrastructure.

Service Oriented Architecture (SOA) **–** An architectural approach that presents a set of reusable software components that align with an agency's business goals and the state's strategic objectives. The services are highly cohesive, loosely coupled, discoverable software components that are decoupled from hardware and network dependencies and that encapsulate the complexities of the underlying implementation.

Service Set Identifier (SSID) – A unique identifier attached to the header of packets sent over a Standard IEEE 802.11 wireless network that acts as a password when a mobile device attempts to connect. The SSID differentiates one wireless network from another, so all devices attempting to connect to a specific wireless network must use the same SSID. Other terms for SSID include network name, preferred network, ESSID, and Wireless LAN Service Area.

Session Key – In the context of symmetric key encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

Shared Source – A situation in which a private community of users has a formal or informal agreement to share software source code. The originating user usually has responsibility over the source code he has provided. There is usually one member, however, who has control over the library of source code and the coordination of version control and membership. There is typically one community license agreement to which the entire membership subscribes and covers all

source code submitted. Additionally, there is usually a memorandum of understanding (MOU) or terms and conditions document that governs behavior (quality assurance, testing, etc.) of contributors.

Shareware – Software that is distributed free on a trial basis where the user is typically required to pay for it after a built-in expiration date or to fully enable features and functionality. *See*, Liteware.

Simple Network Management Protocol (SNMP) – The protocol governing network management and the monitoring of network devices and their functions, including gathering data about network traffic and the behavior of network components. A set of protocols for managing complex networks.

Simulation – A model that behaves like the proposed system.

Sizing – The process of estimating time at a relatively low level of confidence.

Slack – *See,* float.

Skype – A peer to peer (P2P) software application that allows voice calls to be made over the Internet from a personal computer, laptop and other mobile devices. Voice calls may also be made from the application to traditional landline and cellular phones. The software application also provides instant messaging, file transfer and video conferencing.

Smartcard – A tamper-resistant computer chip embedded in a credit card sized card.

Simple Network Management Protocol (SNMP) – A standard for gathering data about network traffic and the behavior of network components.

Social Engineering – 1) A non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures, *e.g.*, theft, trickery, coercion, to steal passwords, keys, user IDs, telephone numbers used for remote dial in, and tokens; 2) A term used among hackers and for cracking techniques that rely on weaknesses in human nature rather than software.

Example: A classic scam includes phoning a person who has the required information and posing as a field service technician or a fellow employee with an urgent access problem. The caller will try to trick someone into revealing passwords or other sensitive information like operating systems, logon IDs, server names, application names, etc.

Social Networking – uses web based environments including sites such as Facebook, Twitter, MySpace and LinkedIn that enable users to post information, in order to develop and maintain online relationships. These sites allow a community of users with like interests to communicate.

SOCKS – A protocol that a proxy server can use to accept requests from client users in an agency's network so that it can forward them across the Internet. SOCKS uses sockets to represent and keep track of individual connections. The client side of SOCKS is built into certain Web browsers and the server side can be added to a proxy server.

Software – Computer programs, systems, and the associated documentation that describes them.

Software-as-a-Service (SaaS) – A model of service delivery where one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the provider. In some occasion, there may be different providers, i.e. one provides SaaS, while another provides Infrastructure as a Service. Contracts must include clearly defined roles and responsibilities for security and incident responses.

Software/System Development Life Cycle (SDLC) – A structure imposed on the development of a software product or system, which guides developers through different phases to complete important aspects of the software's development.

Software Development Process – The process by which user needs are translated into a software product.

Software Fault – *See,* Bug.

Software Metric – A standard of measurement. It is a number assigned to a quantifiable concept that relates to a software product or to the process that created it.

Software Product Life Cycle – The set of all events and endeavors that occur within the birth-to-death cycle of a software product.

Software Project Management Plan – The controlling document for managing a software project. The SPMP defines the technical and managerial project functions, activities, and tasks necessary to satisfy the requirements of a software project.

Software Requirements Specifications – General term for the wide variety of paper-based descriptions of a program or system. Usually a document that contains the complete set of business functional requirements.

Spam – Unsolicited bulk commercial electronic mail.

Spamming – The process of sending unsolicited bulk commercial electronic email.

Specification – A detailed formulation, in document form, providing a definitive description of a system for the purpose of developing that system.

Spiral Model – Software development process where constituent activities are performed iteratively until all software requirements are met. (IEEE)

Split Tunneling – a computer networking concept which allows a remote VPN user to access a public network (e.g., the Internet) at the same time that the user is allowed to access resources on the VPN (e.g., a local LAN or WAN), using the same physical network connection.

Spoof – An attempt by an unauthorized entity to gain access to a system by posing as an authorized user. Also, sending messages or e-mail under a false identity.

Spyware – Any technology that aids in gathering information about persons or organizations without their knowledge. On the Internet, where it is sometimes called a spybot or tracking software, spyware is programming that is put in someone's computer to secretly gather information about the user and to relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

Stability – A state of reliability or dependability.

Staffing Plan – The formal, documented, and approved plan that identifies and allocates resources needed to complete the project.

Stakeholder – A person, or people, who will be affected either positively or negatively by project completion.

Standalone Account – A user or system level account that is used for local computer access while the computer is not attached to a network. Standalone accounts are separate from directory or network based accounts.

Standalone Computer – Describes a computer workstation where the computer is not connected to any other device on a network.

Standard – An approved, documented, and available set of criteria used to determine the adequacy of an action or object.

Standards / Standard Practice – *See,* Architectural Standard Practice

State Agency/Subscriber – Any public agency using the State Network to access the Internet.

State Data – Data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any agency of State government.

State Information System – Any information technology system operated and/or managed by agencies of the State of North Carolina. Examples of such systems include but are not limited to Web servers, the local area network (LAN), and the mainframe.

State-Issued Device – A device issued by the State to be used for official State duties. Typically these devices are funded by State dollars.

Statement of Work (SOW) – A narrative description of products or services to be supplied under contract.

Statewide Architecture Framework – The Statewide Architecture Framework provides guidance for development, implementation, and integration of business systems, business information, and technology to deliver efficient business capabilities throughout state government. The framework also facilitates enterprise project management and approval, sourcing decision for solutions and technology, and strategic business planning. *See,* Statewide Architecture Framework at https://it.nc.gov/services/it-architecture/statewide-architecture-framework.

Statewide Critical – From an information technology perspective, in the agency's opinion, the loss of this application will have a direct impact to statewide core functions, processes and/or activities. The application's loss may also impact a large portion of the State's population.

Statewide Information Security Manual – An enterprise wide set of security standards for state information technology, adopted pursuant to G.S. § 143B-1376, to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. The security standards must be established by the State CIO.

State Network – The integrated information network operated by DIT on behalf of state agencies and other subscribers. For the purpose of the Statewide Information Security Manual, the State Network is considered a public network.

State Network User – Any individual authorized by a public agency/subscriber to use the State Network, including State Network Internet access.

Stateful Inspection – Also referred to as dynamic packet filtering. A firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

Status Report – A management report, sometimes called an activity report, that provides the status of project activities over a period of time,

Strategic Planning – Sets the business and technology direction for an organization by establishing the vision, mission, and objectives based on key stakeholder goals and customer wants and needs.

Streaming Sites – Those Internet sites providing information or data in a continuous stream, such as but not limited to video, audio and tickers (news, weather, stock quotes, sports, etc.). Users who open connections to these types of sites and keep them open utilize a large amount of bandwidth and overall network performance can be degraded.

Stress Test – Testing that ensures that the system performs as expected under a high volume of transactions, high number of users. Sometimes called load testing.

Subcontract – Delegating tasks or sub-projects to contractors or other organizations.

Symmetric Key Cryptography – A form of cryptography in which the same key is used for encrypting and decrypting. This key is generally known by both senders and receivers and must be kept private by the parties. Contrasted to Asymmetric Key or Public Key Cryptography.

Syslog – The system logging facility for Unix systems. It is also commonly used by firewalls and network devices to send audit log data. Syslog uses the UDP protocol used for transmission of data.

System – An assembly of components (hardware, software, procedures, human functions and other resources) united by some form of regulated interaction to form an organized whole. A group of related processes.

System Administrator – An individual responsible for maintaining a multi-user computer system, including a local-area network (LAN).

System Design – The process of defining the hardware and software architecture for a system to satisfy specified requirements.

System Design Review – A review conducted to evaluate the manner in which requirements for a system have been allocated to configuration items. (IEEE)

System Integration – The activities involved in assembling hardware / software components into a deliverable product.

System Requirements Review – A review conducted to evaluate the completeness and adequacy of the defined requirements. (IEEE)

System Test – The final stage of testing on a completed project (prior to client acceptance test) when all hardware and software components are put together and tested as a whole.

Systems Integration Domain – Specifies how various systems, operating on different platforms and/or in external environments, can effectively work together to seamlessly exchange data over various communication systems, thus maximizing system resources.

T

TCO – Total Cost of Ownership

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol over Internet Protocol

THIRA – Threat and Hazard Identification and Risk Assessment

TKIP – Temporal Key Integrity Protocol

TCP Wrapper – A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

Tactical Plan – Specific improvements, or changes, that will be carried out in a fairly short time span (usually twelve (12) months).

Task – A discreet, identifiable, meaningful, and cohesive component (unit) of work on a project (usually 40 to 80 hours of effort). This is the smallest measurable unit of work producing a deliverable and is the lowest level of work on a project.

Task Description – A description that defines all the work required to complete a project task or activity including input, output, expected results, and quality specifications.

Technical Security Architecture – A foundational blueprint document that describes and illustrates the technologies and technology implementation techniques used to obtain a specified level of assurance for the state's information and information resources.

Technical Standard – A technical specification issued by IEEE or other technology standards bodies. When a technical standard related to security has been established by the State, it becomes a security standard.

Techniques – Technical and managerial procedures that aid in the evaluation and improvement of the software development process. (IEEE)

Technology Domain – set of principles and standards that guide the selection, design, and application of related technologies in a specifically defined logical technology domain. Currently defined Statewide Architecture Framework domains include – Application, Data, Enterprise Management, Collaboration, Network, Platform, Security, and Systems Integration.

Techno-Vandalism – A term used to describe a hacker who breaks into a computer system with the sole intent of defacing and or destroying its contents.

Telework – A work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work. (FEMA)

Test – An activity in which a component is executed under specified conditions with the results observed and recorded. (IEEE)

Test Plan – A formal, documented, and approved plan that describes the scope, approach, resources, and schedule of intended test activities.

Test Phase – The period of time in the software life cycle during which the software product is evaluated and integrated to determine if requirements have been met. (IEEE)

Tests, Training, and Exercises (TT&E) – Measures to ensure that an organization's Continuity plan is capable of supporting the continued execution of the organization's Essential Functions throughout the duration of a Continuity event. TT&E activities are designed to familiarize, impart skills and ensure viability of Continuity plans. (FEMA)

Testing – The process of exercising, or evaluating, software by manual or automated means to demonstrate that the software satisfies specified requirements or to identify differences between expected and actual results. It is also the set of defect removal tasks that include execution of all, or part, of an application on a computer.

Test Specifications – A document that prescribes the process and procedures to be used to verify that a product meets the business functional requirements.

Thin client – an n-tier architecture in which most of the computer code is executed on a server and the client process is limited to the user interface only. It provides simplified system management because there is little or no code distributed to other machines.

Third Party Contractors – Non-state employees, such as vendors, suppliers, individuals, contractors, and consultants, including their employees and agents, responsible for providing goods or services to the state.

Threat – An intentional or accidental action, activity or event that can adversely impact agency information assets, as well as the sources, such as the individuals, groups, or organizations, of these events and activities.

Threat and Hazard Identification and Risk Assessment (THIRA) – A three-step risk assessment process of the Department of Homeland Security (DHS) that helps communities answer the following questions:

- What threats and hazards can affect our community?
- If they occurred, what impacts would those threats and hazards have on our community?

- Based on those impacts, what capabilities should our community have?

The THIRA helps communities understand their risks and determine the level of capability they need to address those risks. The outputs form this process lay the foundation for determining a community's capability gaps as part of the Stakeholder Preparedness Review.

Tier – An executable software component comprising one portion of an application. A tier typically performs a complete application function. Note: The number of tiers in an application does not refer to the number of platforms on which an application is deployed.

> **Three-tier (3-tier) –** An application in which the code that implements the business rules, user interface, and data access are separate and distinct from each other and constitute tiers respectively. The code within each tier may be tightly coupled but is still independent from the other tiers.
>
> **Two-tier –** An application in which the code that implements the business rules may be tightly coupled to either the code that implements the user interface or to the code that implements data access.

Time Scale – Planned versus actual time needed to complete a task, activity, phase, or project.

Time Out – A parameter related to an event designed to occur at the conclusion of a predetermined elapsed time.

Temporal Key Integrity Protocol (TKIP) – The WPA encryption method. TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism.

Token Card – Small handheld devices that generate one-time passwords.

Total Cost of Ownership (TCO) – The present value of all costs associated with an information technology investment that is incurred over the expected life of the investment.

Traceability – Manual or automated processes and procedures that map all software components from business function requirements through test cases.

Training Plan – The formal, documented, and approved plan that identifies the schedule and users to be trained on use of the program or system.

Transaction – The input / output to a system resulting from a business event.

Transition Plan – A document that specifies how a product is to transition from development to production support.

Transmission Control Protocol (TCP) – A set of rules used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Transmission Control Protocol/Internet Protocol (TCP/IP) – A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

Trigger – Symptom or warning sign that generates action (e.g., risk management). (PMI)

Triple DES – A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

Trojan Horse – A program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.

Trusted Directory – Repository of user IDs and passwords for the purpose of authentication and/or authorization, following approved security standards for directories.

Tunnel – A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a logical point-to-point link - i.e., an OSI layer 2 connection - created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or inter-network layer protocol (such as IP), or in another link layer protocol. Tunneling can move data between computers that use a protocol not supported by the network connecting them.

Two-Factor Authentication – *See,* Multi-Factor Authentication.

U

UDP – User Datagram Protocol

UTM – Unified Threat Management

Unified Threat Management (UTM) – A category of security appliances which integrates a range of security features into a single appliance. UTM appliances combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities into a single platform.

Unit Test – The testing carried out personally by individual programmers on their own code.

Update – Vendor provided changes to software for either improved functionality or repair of known bugs or defects.

Usability – The quality of an application system that enables it to be easily understood and conveniently employed by the user.

User Datagram Protocol (UDP) – A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network. UDP uses the Internet Protocol to get a datagram from one computer to another but does not divide a message into packets (datagrams) and reassemble it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in.

User Manual – A document that represents the information necessary to employ a system. (IEEE)

User / Normal User – A person, system, application or defined group that has been authenticated to an IT system and granted access only to those resources to which he has been granted authorization. It is also any individual or application that accesses the State Network.

User ID – The identifier by which a person or entity is recognized.

User Testing – Testing process in which the user community, rather than the developer, performs the tests.

User Access – Access to applications by users for non-administrative purposes.

Utility Program – A system program designed to perform a common task.

V

VPN – Virtual Private Network

Validation – The process of evaluating software to assure that the "right product has been built"; that is, to assure that it meets functional and performance requirements (completeness).

Value Analysis – An activity devoted to optimizing cost performance. The systematic use of techniques that identify the required functions, establish values for the functions, and provide the functions at the lowest overall cost without loss of performance.

Vendor Access – Access to the State Network by a non-State entity doing business with the State.

Verification – The process that assures that the software has been "built right", that is, each intermediate product meets specific requirements (correctness).

Verification and Validation – The process of determining whether the requirements for a system are complete and correct. (IEEE)

Virtual LAN – a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN.

Virtual Machine (Guest) – In operating systems, the primary component of a virtualized architecture that serves to replace a traditional physical system or set of systems. Because virtual machines (VMs) are logically separated from the physical resources they use, the host environment is often able to dynamically assign resources among the VMs.

The VM has a traditional OS installed within it that is called the guest OS. This guest OS communicates with a virtual machine host software component which manages the interaction of the OS with the hardware. Depending on the virtualization solution, the host software component may be called a "Virtual Machine Monitor" (VMM) or "Hypervisor." One of the key characteristics of most VMs is that they operate exactly like their physical counterparts so that not only do users experience the same look and feel, but also the system's software programs do not recognize that they are operating within a VM.

Virtual Machine Host – A component of a virtualized environment that performs the intelligent processing of a virtualization solution. It operates between the Virtual Machine (VM) and the hardware and performs the translation between the operating system in the VM and the low-level device drivers. Depending on the virtualization solution, this software component is sometimes referred to as the "Virtual Machine Monitor (VMM)" or "Hypervisor." It provides all of the virtual machine processes and has all of the device drivers.

Virtual Machine Monitor (VMM) – *See*, Virtual Machine Host.

Virtual Network – An interconnected group of virtual machines configured to use a network adapter in the physical computer or no network adapter.

Virtual Private Network (VPN) – A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if an agency has LANs at several different sites, each connected to the Internet by a firewall, the agency could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally

less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

1. **Gateway-to-Gateway VPN** – Provides connectivity and security between a branch or partner office to the central site system.

2. **Client-to-Gateway VPN** – Provides connectivity and security between a remote client machine and the central site system.

Virtual Switch – The network conduit among the virtual network interface cards of a Virtual Machine (VM), other VMs on the same physical host, and the physical network where it binds to the physical network interface cards (NICs) on a machine. The Virtual Switch provides the same services as a physical switch. Every VM that is configured for network communications has a virtual network device driver that sends packets to the virtual switch.

Virus – Computer viruses, Trojan Horses, worms or other destructive computer programs.

Vulnerability – A weakness in an information technology system, system security procedures, internal controls, or implementation that could be exploited.

Vulnerability Assessment – An evaluation of the current security posture and is intended to reveal security related control strengths and control weaknesses.

The systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

1. **Network Based Vulnerability Tools** – Perform analyses of an enterprise's critical network and system infrastructure from the view of an intruder trying to use the network to break into systems. The tools often replicate techniques used to exploit remote systems. Network scanners are comprised of a collection of various tools to examine common vulnerabilities.

2. **Host Based Vulnerability Tools –** Look specifically at a host's vulnerabilities.

Vulnerability Mitigation – The action taken to reduce the risk of the vulnerability.

Vulnerability Risk Ratings – The risk ratings assigned to a vulnerability are as follows:

1. **High-level Risk:** A vulnerability that could cause grave consequences if not addressed and remedied immediately. This type of vulnerability is present within the most sensitive portions of the network, as identified by the data owner. This vulnerability could cause network functionality to cease or control of the network to be gained by an intruder.

2. **Medium-level Risk:** A vulnerability that should be addressed within the near future. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner.

3. **Low-level Risk:** A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network to be exploited and/or it is of little consequence to the data owner. Vulnerabilities of this nature are common among most networks and usually involve a simple patch to remedy the problem. These patches can also be defined as enhancements to the network.

W

WAN – Wide Area Network

WAP – Wired Application Protocol

WBS – Work Breakdown Structure

WEP – Wired Equivalent Privacy

WDC – Western North Carolina Data Center

WPA – Wi-Fi Protected Access

WTLS – Wireless Transport Layer Security

WWW – World Wide Web

Walkthrough – A software inspection process, conducted by peers, to evaluate the software element.

Waterfall Model – A software development life cycle approach developed by Winston W. Royce that partitions a project into manageable phases (requirements, design, implementation, and test).

Web-based – A system that runs on the Web or on Internet-based networks such as an intranet. Users typically access systems that are web-based through a browser.

Web-centric – describes a computing environment where most of the presentation and business logic is contained on the client side of a web-enabled application. This is not consistent with the Statewide Architecture Framework or with accepted industry practice.

Web-enabled – *See*, Web-based.

Web Server – a software program (that runs on a physical server) that processes protocols such as HTML and XML using the Hyper Text Transfer Protocol (http) daemon or service to send and receive web pages (and any associated data/files) from a user on the Internet via the World Wide Web.

Web Services – describes a standardized way of integrating Web-based applications using open standard interfaces over an Internet protocol backbone. Used for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

White Box Testing – Testing that verifies that specific lines of code work as specified.

Wide Area Network (WAN) – A data telecommunications network typically extending a LAN outside a building, over common carrier lines, to link to other LANs that are geographically dispersed. In some situations, point-to-point wireless access points can be used to replace the common carrier lines.

Wired Equivalent Privacy (WEP) – A security protocol for wireless networks defined in the IEEE 802.11 standard. WEP provides security by encrypting data over the radio waves as it is transmitted from one end point to another in a wireless LAN, *i.e.*, from access point to laptop. WEP has been superseded by more secure wireless protocols and it should not be used.

Wi-Fi Protected Access (WPA) – A vendor consortium agreement based on an early draft of 802.11i for secure wireless LAN implementation. The agreement covers using TKIP to enhance wireless encryption and security by implementing message integrity checks, better initialization vectors and dynamic keys. WPA also provides for 802.1X authentication.

Wi-Fi Protected Access version 2 (WPA2) (IEEE 802.11i Robust Network Security) – IEEE standard for secure wireless LAN implementation. The standard is a collection of security features, like IEEE 802.1X, not a single solution in itself.

Wireless Application Protocol (WAP) – A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat (IRC).

Wireless Devices – Any device, including laptops and personal computers with wireless network interface cards that can connect to the State Network.

Wireless LAN Gateway – An intermediary device designed to provide segmentation of the wireless LAN from the wired LAN. Such devices include routers, firewalls, and network switches capable of providing VLAN segmentation.

Wireless Mesh Network – A wireless mesh network (WMN) provides communication between nodes over multiple access points (AP) on a full or partial mesh topology. In an infrastructure mesh configuration, the WMN uses wireless links (peer radio devices that don't have to be wired

to a wired port like traditional APs do) to provide a data path from unwired fixed access points to other unwired APs or back to an access point that has a connection to a wired network. The nodes basically act as routers, using a wireless mesh routing protocol to establish frame-forwarding paths through the mesh.

Wireless Transport Layer Security (WTLS) – The security layer of WAP, providing privacy, integrity and authentication for WAP services.

Work Breakdown Structure (WBS) – A task oriented family tree of phases, activities, and tasks that organizes, defines, and graphically displays the total work to be accomplished.

Work Package – A specification for the work to be accomplished in completing an activity or task. It is also a deliverable at the lowest level of the work breakdown structure.

Work Product – Any tangible item that results from a project function, activity, or task.

Workstation – Any machine with all of its installed storage, processing, and communications that can be either standalone or networked.

World Wide Web (WWW) – The integrated worldwide network of computers based on the hypertext transfer protocol (HTTP) and Transmission Control Protocol/Internet Protocol (TCP/IP), commonly used to bring information to computer users via a client browser program.

Worm – A self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

X

Y

Z

Zone – *See*, Domain Name System (DNS) Zone or Network Zone.

Zone Transfer – The process of transferring a complete copy of the data from one zone from a DNS server to another machine. Typically, the process includes a Secondary DNS server updating its Zone data by querying the Zone data from the Primary DNS Server.