BUSINESS AND IT/IRM

GLOSSARY, ACRONYMS & REFERENCE GUIDE

TABLE OF CONTENTS

1. FORWARD

The Office of Information Management and Technology (OIMT) implemented State of Hawai'i Business and Information Technology (IT) and Information Resource Management (IRM) Glossary, Acronyms, and Reference Guide, dated July 2012, as a standalone document for assisting in development of documentation related to IT/IRM and business processes.

This guide is intended to be a companion document in collaboration with the Office of Information Management & Technology Business IT/IRM Transformation Plan to restructure the business processes and information technologies serving the employees and citizens of the State of Hawai'i.

Most of the terms in this document are derived from various federal, state, local, educational and private sector sources, but a number of them have been examined for consistency in order to remove inconsistencies among the departments and the State IT & business community.

This glossary, acronyms and reference document is intended to fulfill several overall objectives:

- Resolve differences between the definitions of terms used by the State, Local, Federal to enable all departments to use the same source of information (and move towards shared documentation and processes).
- Accommodate the transition from multiple information technology organizations to a single statewide information technology organization in current use to the terms now appearing in documents produced by the State IT Transformation initiative.
- Ensure consistency among related and dependent terms.
- Identify terms and acronyms which have multiple meanings depending on the situation or document(s) where the term or acronym appears
- Include terms that are important to the support of goals of State Departments and to the concept of information sharing.
- Review existing definitions to reflect, as appropriate a broader enterprise perspective vice a system perspective.
- Strike an appropriate balance between macro terms and micro terms (i.e., include terms that are useful in writing and understanding documents dealing with business or IT/IRM policies, directives, instructions, and guidance, and strike terms that are useful only to specific business or IT/IRM subspecialties).

Many technology and business terms come and go into vogue and OIMT has attempted to include significant examples that have a useful distinction when compared to existing Information Assurance terms. A number of terms recommended for inclusion in the glossary were not added – often because they appeared to have a narrow application.

When glossary terms have common acronyms, they have been noted the acronym with the term and added the acronym to the acronym list. In some instances, there may be several meanings for the same acronym, and in those cases OIMT has tried to list all the common meanings. Note that some acronyms are self-explanatory, and so there is no definition of these acronyms in the glossary itself.

OIMT is creating this document has attempted to include as many information technology and information assurance definitions, many other terms have been overlooked for a specific reasons or were simply overlooked, or not relevant, and some terms are newly identified, If there is a term or definition that is either not included in this glossary or should be identified as a Candidate For Deletion (C.F.D.) in future versions of this document, please submit the term with a definition based on the following criteria: 1) specific relevance to Information Assurance; 2) economy of words; 3) accuracy; 4) broad applicability; and 5) clarity. Use these same criteria to recommend any changes to existing definitions or to suggest new terms (definitions must be included with any new terms). When recommending a change to an existing definition, please note how that change might affect other terms. In all cases, send your suggestions to the State of Hawai'i Office of Information Management & Technology via e-mail address listed below.

OIMT recognizes that, to remain useful, a glossary must be in a continuous state of coordination, and encourages reviews and welcome comments as new terms become significant and old terms fall into disuse or change meaning. The goal of OIMT is to keep this document relevant and a useful tool for commonality among the State's IT community.

State of Hawai'i
Office of Information Management and Technology

RE: Business and IT/IRM – Glossary, Acronyms &
Reference Guide

mailto: oimt@hawaii.gov

2. GLOSSARY

This instruction applies to all State of Hawai‘i Executive Branch Departments, Agencies, Divisions, Bureaus and Offices; supporting contractors and agents; that collect, generate process, store, display, transmit or receive state sensitive information or that operate, use, or connect to the State managed Network or information technology systems, as defined herein. Private industry, educational institutions, citizens, etc. can use the terms and acronyms herein as a guideline when dealing with the State's IT/IRM infrastructure or reference documentation.

0 – 9

3rd Generation (3G) – used to represent the 3rd generation of mobile telecommunications technology. This is a set of standards used for mobile devices and mobile telecommunication services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.[1] 3G finds application in wireless voice telephony, mobile Internet access, Fixed Wireless Internet access, video calls and mobile TV.

4th Generation (4G) – 4G is the fourth generation of cell phone mobile communications standards. It is a successor of the third generation (3G) standards. A 4G system provides mobile ultra-broadband Internet access, for example to laptops with USB wireless modems, to smartphones, and to other mobile devices. Conceivable applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing and 3D television.

6 Sigma (6σ) – A widely used business management strategy, originally developed by Motorola during the 1980s, made popular by Jack Welch at General Electric during the 1990s. 6 Sigma attempts to improve the quality of the outputs of a process by identifying and removing the causes of errors and minimizing the variability in manufacturing and business processes. (See also Lean Six Sigma.)

A

access – Opportunity to make use of an information system (IS) resource.

access control – Limiting access to information system resources only to authorized users, programs, processes, or other systems.

Access Control List (ACL) – 1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

access list – Roster of individuals authorized admittance to a controlled area.

accountability – Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

accreditation - Formal declaration by State Authorized Accrediting Authority (SAAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

[1] *Clint Smith, Daniel Collins. "3G Wireless Networks", page 136. 2000.*

Accrediting Authority – Synonymous with Designated Accrediting Authority (DAA). See also Authorizing Official.

accreditation package – Product comprised of a System Security Plan (SSP) and a report documenting the basis for the accreditation decision.

Active Directory (AD) – A directory service created by Microsoft for Windows domain networks. It is included in most Windows Server operating systems.

Active Directory provides a central location for network administration and security. Server computers that run Active Directory are called domain controllers. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.[2]

Advanced Encryption Standard (AES) – A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Advanced Persistent Threat (APT) – Refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information[3], but applies equally to other threats such as that of traditional espionage or attack.[4] Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.[5]

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

Agile – Refers to software development as a group methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development cycle. The Agile Manifesto[6] introduced the term in 2001.

air-gapped system – Two or more computer systems that are physically, electrically, and electromagnetically isolated from one another, in order to create a more secure set of systems.

applet – Any small application that performs one specific task within the scope of a larger program, often as a plug-in.

application – Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

[2] *"Active Directory on a Windows Server 2003 Network". Active Directory Collection. Microsoft. 13 March 2003. http://technet.microsoft.com/en-us/library/cc780036(WS.10).aspx#w2k3tr_ad_over_qbjd. Retrieved 20 July 2012.*

[3] *"Anatomy of an Advanced Persistent Threat (ATP)". Dell SecureWorks. http://go.secureworks.com/advancedthreats. Retrieved 21 July 2012.*

[4] *"Are you being targeted by an Advanced Persistent Threat?". Command Five Pty Ltd. http://www.commandfive.com/apt.html. Retrieved 21 July 2012.*

[5] *"The changing threat environment...". Command Five Pty Ltd. http://www.commandfive.com/threats.html. Retrieved 21 July 2012.*

Approval to Operate (ATO) – The official management decision issued by a SAAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

anti forensics –

asset – A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. (see also – investment, portfolio)

assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

attack – Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

audit – Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

audit log – A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

audit reduction tools – Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.

audit trail – A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.

authenticate – To verify the identity of a user, user device, or other entity.

authentication – The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

authenticator – The means used to confirm the identity of a user, process, or device (e.g., user password or token).

uthenticity – The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
See Authentication.

authorization – Access privileges granted to a user, program, or process or the act of granting those privileges.

availability – The property of being accessible and useable upon demand by an authorized entity. Ensuring timely and reliable access to and use of information.

Average Rate of Occurrence (ARO) – The annualized rate at which a particular event or incident occurs. Used in qualitative risk management, in order to develop a risk assessment.

B

back door – Typically unauthorized hidden software or hardware mechanism used to circumvent security controls.

backup – Copy of files and programs made to facilitate recovery, if necessary.

banner – Display on an information system that sets parameters for system or data use.

baseline – Hardware, software, databases, and relevant documentation for an information system at a given point in time.

biometrics – Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

blended attack – A hostile action to spread malicious code via multiple methods.

bot – Modified term for “robot”, is a compromised computer system on the Internet which is being used as part of an overall ‘botnet’ to perform attacks against other Internet resources, but hides the identity of the actual attacker.

botnet – A botnet is a collection of compromised computers connected to the Internet (each compromised computer is known as a ‘bot’). When a computer is compromised by an attacker, there is often code within the malware that commands it to become part of a botnet.

boundary – Physical or logical perimeter of a system.

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

breach – A breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

buffer overflow – A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Business Continuity Plan (BCP) – The documentation of a predetermined set of instructions or procedures that describe how an organization’s business functions will be sustained during and after a significant disruption.

Business Impact Analysis (BIA) – The documentation of a predetermined set of instructions or procedures that describe how an organization’s business functions will be sustained during and after a significant disruption.

Business Process Reengineering (BPR) – A business management strategy originally pioneered in the early 1990s, focusing on the analysis and design of workflows and processes within an organization. BPR aimed to help organizations fundamentally rethink how they do their work in order to dramatically improve customer service, cut operational costs, and become world-class competitors. In the mid-1990s, as many as 60% of the Fortune 500 companies claimed to either have initiated reengineering efforts, or to have plans to do so.

C

Certificate – A digitally signed representation of information that

1) identifies the authority issuing it
2) identifies the subscriber
3) Identifies its valid operational period (date issued / expiration date).

community certificate usually implies public key certificate and can have the following types:

1) cross certificate; 2) encryption certificate; & 3) identity certificate

Certificate management – Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.

Certificate Policy (CP) – A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate Revocation List (CRL) – A list of revoked public key certificates created and digitally signed by a Certification Authority.

Certificate Status Authority (CSA) – A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

chain of custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

chain of evidence – A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.

ciphertext – Is the result of encryption performed on plaintext using an algorithm, called a cipher. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it.

clearing – The removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities. The data may still be recoverable, but not without special laboratory techniques.

Clearing is typically an administrative protection against accidental disclosure within an organization. For example, before a hard drive is re-used within an organization, its contents may be cleared to prevent their accidental disclosure to the next user.

cloud computing – A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS)); and four models for enterprise access (Private cloud, Community cloud, Public cloud and Hybrid cloud).
Note: Both the user's data and essential security services may reside in and be managed within the network cloud.

coeverity – The level of magnetic field used to read/write data to a data storage device.

cold site – Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services.

Common Vulnerabilities and Exposures (CVE) – A dictionary of common names for publicly known information system vulnerabilities.

compensating security control – A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

compromise – Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

computer cryptography – Use of a crypto-algorithm program by a computer to authenticate or encrypt/ decrypt information.

Computer Forensics – The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Computer Network Attack (CNA) – Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND) – Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

Computer Network Exploitation (CNE) – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

Computer Security – Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

computer security incident – See Incident.

Computer Security Incident Response Team (CSIRT) – Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability or Cyber Incident Response Team).

computer security object – A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects.

computer security subsystem – Hardware/software designed to provide computer security features in a larger system environment.

computing environment – Workstation or server (host) and its operating system, peripherals, and applications.

confidentiality – The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

configuration control – Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation.

Configuration Control Board (CCB) – A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational lifecycle of an information system.

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

Continuity of Government (COG) – A coordinated effort within the Federal Government's executive branch to ensure that national essential functions continue to be performed during a catastrophic emergency.

Continuity of Operations Plan (COOP) – Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan.

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

controlled access area – Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance.

controlled interface – A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.

cookie – Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.

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

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

credential – Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.

critical infrastructure – System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

cross-certificate – A certificate used to establish a trust relationship between two Certification Authorities.

cracker – Cracking is the act of breaking into a computer system, often on a network. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. See hacker.

cross certificate – A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two Cas.

cryptography – Art or science concerning the principles means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

cryptology – The mathematical science that deals with cryptanalysis and cryptography.

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

cyber cartel – A criminal organization developed with the primary purpose of promoting, controlling and profiting from the exploitation of individuals and computer systems on the Internet.

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber-attacks.

cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

D

data – A subset of information in an electronic format that allows it to be retrieved or transmitted.

data asset –
1. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset.
2. An information-based resource.

data integrity – The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Data At Rest (DAR) – The term used to describe all data in storage but excludes any data that frequently traverses the network or that which resides in temporary memory. Data at rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, USB thumb drives, files stored on backup tape and disks, and also files stored off-site or on a storage area network (SAN).

Data In Motion (DIM) – Is data being transferred between two nodes in a network. This data can be regarded as secure if and only if (a) both hosts are capable of protecting the data in the previous two classifications and (b) the communication between the two hosts is identified, authenticated, authorized, and private, meaning no third host can eavesdrop on the communication between the two hosts.

Data In Use (DIU) – Is data not in an at rest state, that is on only one particular node in a network (for example, in resident memory, or swap, or processor cache or disk cache, etc. memory). This data can be regarded as “secure” if and only if (a) access to the memory is rigorously controlled (the process that accessed the data off of the storage media and read the data into memory is the only process that has access to the memory, and no other process can either access the data in memory, or man-in-the-middle the data while it passes through I/O), and (b) regardless of how the process terminates (either by successful completion, or killing of the process, or shutdown of the computer), the data cannot be retrieved from any location other than the original at rest state, requiring re-authorization.

data loss – Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or restore lost data.

Data Loss Prevention (DLP) – Refers to systems that identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination and so on) and with a centralized management framework. Systems are designed to detect and prevent unauthorized use and transmission of confidential information.
(See also data in use, data in motion and data at rest.)

Data owner – The head of the organization that has final statutory and operational authority for specified information. (In the government community, the Data Owner is usually the department head who establishes the controls used for the collection, processing, and dissemination of specified information.)

decrypt – Generic term encompassing decodes and decipher.

Defense-in-Breadth – A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Defense-in-Depth – Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

degauss – Procedure to reduce the magnetic field on a data storage device (E.g. hard disk drive) to virtual zero by applying a reverse magnetizing field.
Also called demagnetizing.

deleted file – A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data.

Demilitarized Zone (DMZ) – Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network’s Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Denial of Service (DoS) – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Disaster Recovery Plan (DRP) – Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan.

Discretionary Access Control (DAC) – A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

disruption – An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Distributed Denial of Service (DdoS) – A Denial of Service technique that uses numerous hosts to perform the attack.

Domain Name Service (DNS) – A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various pieces of information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

Domain Name Service Security Extensions (DNSSEC) – A suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

dumpster diving – The practice of sifting through commercial or residential trash containers to find items of useful in identity theft, social engineering, or for items of value that have been discarded without proper destruction of the information contained.

E

electronic signature – The process of applying any mark in electronic form with the intent to sign a data object. (See also digital signature.)

enclave – Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

encryption – The process of changing plaintext into ciphertext for the purpose of security or privacy.

encryption certificate – A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate. (See also certificate)

end-to-end encryption – Encryption of information at its origin and decryption at its intended destination without intermediate decryption.

end-to-end security – Safeguarding information in an information system from point of origin to point of destination.

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

Enterprise Resource Planning (ERP) – A system(s) integrating internal and external management information across an entire organization, embracing finance/accounting, manufacturing, asset management, sales and service, customer relationship management, etc. ERP systems automate this activity with an integrated software application. The purpose of ERP is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders.

enterprise risk management – The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.

Evaluation Assurance Level (EAL) – Set of assurance requirements that represent a point on the Common Criteria predefined assurance scale.

event – Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

external information system – An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

extranet – A private network that uses Web technology, permitting the sharing of portions of an enterprise's information or operations with suppliers, vendors, partners, customers, or other enterprises.

F

failover – The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

false acceptance – In biometrics, the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out.

False Acceptance Rate (FAR) – The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

false rejection – In biometrics, the instance of a security system failing to verify or identify an authorized person. It does not necessarily indicate a flaw in the biometric system; for example, in a fingerprint-based system, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorized user.

False Rejection Rate (FRR) – The measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's false rejection rate typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

Federal Information Processing Standard (FIPS) – A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Federal Information Security Management Act (FISMA) – A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB.

file protection – Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.

firewall – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

flooding – An attack that attempts to cause a failure in a system by providing more input than the system can process properly.

forensics copy – An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.

forensics – The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

File Transfer Protocol (FTP) – A standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

fault tolerant – The property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naïvely-designed system in which even a small failure can cause total breakdown. Fault-tolerance is particularly sought-after in high-availability or life-critical systems.

G

gateway – Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

general user – An authorized user of a computer, system or application. General users make up the largest portion of all users of system; general users are granted the concept of least-privilege and are only granted access to systems and data in order to perform normal work duties.

General Users Guide (GUG) – A set of standards, guidelines and procedures used by general users of a computer system to perform their daily work assignments.

Global Information Grid (GIG) – The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

group authenticator – Used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group.

Guard (system) – A mechanism limiting the exchange of information between information systems or subsystems.

H

hacker – Unauthorized user who attempts to or gains access to an information system.

Hacktivism – (a morphing of the words of hack and activism) is the use of computers and computer networks as a means of protest to promote political ends. The term was first coined in 1996 by a member of the Cult of the Dead Cow hacker collective named Omega. If hacking as “illegally breaking into computers” is assumed, then hacktivism could be defined as “the use of legal and/or illegal digital tools in pursuit of political ends”. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, typosquatting and virtual sabotage. If hacking as “clever computer usage/programming” is assumed, then hacktivism could be understood as the writing of code to promote political ideology: promoting expressive politics, free speech, human rights, and information ethics through software development. Acts of hacktivism are carried out in the belief that proper use of code will be able to produce similar results to those produced by regular activism or civil disobedience.

hacktivist – An individual who uses computers and computer networks as a means of protest to promote political ends.

hardware – The physical components of an information system.

Health Information Privacy Accountability Act(HIPAA) – Federal legislation enacted on August 21, 1996 by the United States Congress. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

high impact – The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.)

high-impact system – An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high.

honeypot – A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.

honeynet – A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker’s activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and “trap” people who attempt to penetrate other people’s computer systems. Although the primary purpose of a honeynet is to gather information about attackers’ methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources.

hot site – Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization.

Hypertext Markup Language (HTML) – The main markup languages for creation of web pages, the elements of HTML are the basic building blocks of webpages.

Hypertext Transfer Protocol (HTTP) – Is the application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext Transfer Protocol Secure (HTTPS) – Is the combination of Hypertext Transfer Protocol (HTTP) with SSL protocol. It provides encrypted communication and secure identification of a network web server.

identification – An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.

identifier – A data object – often, a printable, non-blank character string – that definitively represents a specific identity of a system entity, distinguishing that identity from all others.

identity – The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

identity token – Smart card, metal key, or other physical object used to authenticate identity.

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

identity certificate – A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures. (See also certificate.)

impact level – The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

inadvertent disclosure – Type of incident involving accidental exposure of information to an individual not authorized access.

incident – An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

incident response plan – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).

indicator – Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

individual accountability – Ability to associate positively the identity of a user with the time, method, and degree of access to an information system.

information – Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security which in turn grew out of practices and procedures of computer security.

Information Assurance Vulnerability Alert (IAVA) – Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.

IA architecture – A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

IA infrastructure – The underlying security framework that lies beyond an enterprise's defined boundary, but supports its IA and IA-enabled products, its security posture and its risk management plan.

Industrial Control System (ICS) – A term describing the control systems used in industrial production. E.g. Power, water or manufacturing systems. (See also Supervisory Control and Data Acquisition.)

Information Resources Management (IRM) – The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies.

Information Security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

information security policy – Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Information System (IS) – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

information system life cycle – The phases through which an information system passes, typically characterized as initiation, development, operation, and termination (i.e., sanitization, disposal and/or destruction).

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Infrastructure As A Service (IaaS) – Delivers cloud computer infrastructure services, typically in the form of platform virtualization environments. A customer purchase services in the form of a utility and includes all resources necessary to satisfy client computing requirements.

inside acquisition threat – An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

integrity – The property whereby an entity has not been modified in an unauthorized manner.

intellectual property – Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract "properties" has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.

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

interface – Common boundary between independent systems or modules where interactions take place.

internal network – A network where 1) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or 2) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

internal security controls – Hardware, firmware, or software features within an information system that restrict access to resources to only authorized subjects.

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

Internet Protocol (IP) – Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

intranet – A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency).

intrusion – Unauthorized act of bypassing the security mechanisms of a system.

Intrusion Detection Systems (IDS) – Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations).

Intrusion Detection Systems (IDS) (host-based) – IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Intrusion Detection Systems (IDS) (network-based) – IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Intrusion Prevention System (IPS) – System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

IP Security (IPSEC) – Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPSec also includes protocols for cryptographic key establishment.

IT Security awareness and training program – Explains proper rules of behavior for the use of agency information systems and information. The program communicates IT security policies and procedures that need to be followed.

J

K

keystroke monitoring – The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

L

label – See Security Label

labeled security protections – Access control protection features of a system that use security labels to make access control decisions.

Lean Six Sigma – A synergized managerial concept of Lean and Six Sigma that results in the elimination of the seven kinds of wastes (classified as Defects, Overproduction, Transportation, Waiting, Inventory, Motion and Over-Processing) and provision of goods and service at a rate of 3.4 defects per million opportunities (DPMO) .

The Lean Six Sigma concepts were first published in the book titled "Lean Six Sigma: Combining Six Sigma with Lean Speed" authored by Michael George in the year 2002. Lean Six Sigma utilizes the DMAIC phases similar to that of Six Sigma. The Lean Six Sigma projects comprise the Lean's waste elimination projects and the Six Sigma projects based on the critical to quality characteristics. The DMAIC toolkit of Lean Six Sigma comprises all the Lean and Six Sigma tools. The training for Lean Six Sigma is provided through the belt based training system similar to that of Six Sigma. The belt personnel are designated as White Belts, Yellow Belts, Green Belts, Black Belts and Master Black Belts. See also Six Sigma

least privilege – The principle that security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

least trust – The principal that security architecture should be designed in a way that minimizes 1) the number of components that require trust and 2) the extent to which each component is trusted.

likelihood of occurrence – In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.

local access – Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

local authority – Organization responsible for generating and signing user certificates in a PKI-enabled environment.

logic bomb – A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

logical perimeter – A conceptual perimeter that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. Without a reliable human review by an appropriate authority. The location of such a review is commonly referred to as an “air gap.”

Long Term Evolution – A mobile communication standard which allows for higher speeds in the transmission of data and voice to mobile devices such as cellular phones, tablet devices, etc. A standard associated with 3G and 4G communications. See 3rd and 4th Generation.

low impact – The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the interests of the State of Hawai‘I; (i.e., 1) causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2) results in minor damage to organizational assets; 3) results in minor financial loss; or 4) results in minor harm to individuals.

low-impact system – An information system in which all three security properties (i.e., confidentiality, integrity, and availability) are assigned a potential impact value of low.

M

macro virus – A virus that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute and propagate.

magnetic remanence – Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See clearing.

malicious applets – Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system.

malicious code – Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

malicious logic – Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

malware – See malicious code, malicious applets, and malicious logic.

management controls – Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions.

management security controls – The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security.

Mandatory Access Control (MAC) – A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity.

Man-in-the-Middle Attack (MitM) – A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

masquerading – A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.

media – Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

media sanitization – The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Memorandum of Understanding/ Memorandum of Agreement (MOU/MOA) – A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, e.g., establishing, operating, and securing a system interconnection.

message digest – A cryptographic checksum typically generated for a file that can be used to detect changes to the file. Synonymous with hash value/result.

mobile computing – Human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components

mobile code – Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

moderate impact – The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the State of Hawaiʻi; (i.e., 1) causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

moderate impact system – An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

multi-factor authentication – An approach to security authentication, which requires that the user of a system provide more than one form of verification in order to prove their identity and allow access to the system.

Multi-factor authentication takes advantage of a combination of several factors of authentication; three major factors include verification by something a user knows (such as a password), something the user has (such as a smart card or a security token), and something the user is (such as the use of biometrics). Due to their increased complexity, authentication systems using a multi-factor configuration are harder to compromise than ones using a single factor of authentication.
See also strong authentication.

N

National Information Infrastructure (NII) – Nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes both public and private networks, the internet, the public switched network, and cable, wireless, and satellite communications.

National Vulnerability Database (NVD) – The U.S. Government repository of standards based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance (e.g., FISMA).

need-to-know – A method of isolating information resources based on a user’s need to have access to that resource in order to perform their job but no more. The terms ‘need-to know” and “least privilege” express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

need-to-know determination – Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

network – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

network resilience – A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

non-repudiation – Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information.

O

object – Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains.

object reuse – Reassignment and reuse of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.

operational controls – The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Operations Security (OPSEC) – Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

outside acquisition threat – An unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

overt channel – Communications path within a computer system or network designed for the authorized transfer of data. See covert channel.

overwrite procedure – A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns.

P

packet sniffer – Software that observes and records network traffic.

passive attack – An attack that does not alter systems or data.

password – A secret string of letters, numbers and special characters used for accessing information systems. User supplied and maintained.

patch management – The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Payment Card Industry-Data Security Standard (PCI-DSS) – A widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

penetration – See intrusion.

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

perimeter – A perimeter is the boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network.

Personally Identifiable Information (PII) – Information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

As defined in State of Hawai‘i Acts 135 and 136 includes an individual’s first name (or initial) in combination with any one or more of the following additional data elements, in combination, when the all data elements are not sufficiently encrypted.

1. Social Security Number; or
2. Driver’s License number or Hawai‘i identification number; or
3. Account number, credit/debit card number, access code, or password that would permit access to an individual’s financial account. (NOTE: this includes pCard/credit/EBT/debit cards issued to state employees or citizens of the state.)

Personal information does not include publically available information that is lawfully made available to the general public from federal, state or local via governmental records. HRS §487N-1

Personal Identification Number (PIN) – A short numeric code used to confirm identity. Often used in a multi-factor authentication implementation.

phishing – Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means.

plaintext – Unencrypted information.

Plan of Action and Milestones (POA&M) – A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Platform As A Service (PaaS) – A category of cloud computing services that provide a computing platform and a solution stack as a service. In the classic layered model of cloud computing, the PaaS layer lies between the SaaS and the IaaS layers.

PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet.

Post Office Protocol (POP) – An application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

port scanning – Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Portable Electronic Device (PED) – Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

potential impact – The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

precursor – A sign that an attacker may be preparing to cause an incident. See indicator.

Privacy Impact Assessment (PIA) – An analysis of how information is handled 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

privilege – A right granted to an individual, a program, or a process.

privileged account – An information system account with approved authorizations of a privileged user.

privileged command – A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

privileged process – A computer process that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary processes are not authorized to perform.

privileged user – A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Privileged Users Guide (PUG) – document(s) intended to outline approved methodologies used by privileged users in maintaining and monitoring computer systems.

Privileged User Management (PUM) – The function of monitoring privileged access and usage of systems.

probability of occurrence – See likelihood of occurrence.

probe – A technique that attempts to access a system to learn something about the system.

profiling – Measuring the characteristics of expected activity so that changes to it can be more easily identified.

proprietary information – Material and information relating to or associated with the State's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the state as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

protection level (PL) – Based on the Confidentiality of information contained with a system. Each Information System shall incorporate security features that will control the release of information commensurate with the sensitivity of the information being processed, as well as with the established access approval procedures, and need-to-know of the users of the IS, will determine the Protection Level assigned to the IS. For each IS, assurance commensurate with the Protection Level shall be provided.

protection philosophy – Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

protocol – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

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

proxy agent – A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device.

proxy server – A server that services the requests of its clients by forwarding those requests to other servers.

public domain software – Software not protected by copyright laws of any nation that may be freely used without permission of, or payment to, the creator, and that carries no warranties from, or liabilities to the creator.

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

public key certificate – See certificate.

Public Key Cryptography – Encryption system that uses a public-private key pair for encryption and/or digital signature.

Public Key Infrastructure (PKI) – The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

Q

3rd Generation (3G) – The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements.
Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.

R

rapid application development (RAD) – A software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements. See also Agile.t reciprocity – Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

records – In computer science, records (also called tuples, structs, or compound data) are among the simplest data structures. A record is a value that contains other values, typically in fixed number and sequence and typically indexed by names. The elements of records are usually called fields or members.

For example, a date could be stored as a record containing a numeric year field, a month field represented as a string, and a numeric day-of-month field. As another example, a Personnel record might contain a name, a salary, and a rank. As yet another example, a Circle record might contain a center and a radius. In this instance, the center itself might be represented as a Point record containing x and y coordinates.

Records are distinguished from arrays by the fact that their number of fields is typically fixed, each field has a name, and that each field may have a different type.

A record type is a data type that describes such values and variables. Most modern computer languages allow the programmer to define new record types. The definition includes specifying the data type of each field and an identifier (name or label) by which it can be accessed. In type theory, product types (with no field names) are generally preferred due to their simplicity, but proper record types are studied in languages such as System F-sub. Since type-theoretical records may contain first-class function-typed fields in addition to data, they can express many features of object-oriented programming.

Records can exist in any storage medium, including main memory and mass storage devices such as magnetic tapes or hard disks. Records are a fundamental component of most data structures, especially linked data structures. Many computer files are organized as arrays of logical records, often grouped into larger physical records or blocks for efficiency.

records management – The process for tagging information for records keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements.

Registration Authority (RA) – A trusted entity that establishes and vouches for the identity of a subscriber to a Credentials Service Provider (CSP). The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).

remanence – Residual information remaining on storage media after clearing. See magnetic remanence and clearing.

remediation – The act of mitigating vulnerability or a threat.

remote access – Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

removable media – Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device, and is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices.

replay attacks – An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

residual risk – Portion of risk remaining after security measures have been applied.

Risk – 1) Uncertain, unpredictable, or unplanned event that, if occurs, will affect the outcome negatively or positively.; 2) A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of

a. the adverse impacts that would arise if the circumstance or event occurs; and
b. The likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State.

risk assessment – The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

risk management – The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes:

1) the conduct of a risk assessment;
2) the implementation of a risk mitigation strategy;
3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and
4) Documenting the overall risk management program.

Risk Management Framework (RMF) – A structured approach used to oversee and manage risk for an enterprise.

risk mitigation – Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

risk tolerance – The defined impacts to an enterprise's information systems that an entity is willing to accept.

robustness – The ability of an Information Assurance entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.

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

Role-Based Access Control (RBAC) – Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Root Certification Authority – In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

rule-based security policy – A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. Also known as discretionary access control (DAC).

S

safeguards – Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

sandbox – A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

sanitization – A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

scanning – Sending packets or requests to another system to gain information to be used in a subsequent attack.

scavenging – 1. Searching through object residue to acquire data;
2. The act of rummaging through items thrown away in search of sensitive or confidential information. See Social Engineering.

secure communications protocol – A communication protocol that provides the appropriate confidentiality, authentication, and content integrity protection.

Secure Shell (SSH) – A network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network.

Secure Socket Layer (SSL) – A protocol used for protecting private information during transmission via the Internet.
Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:."

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

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

Security As A Service (SaaS) – Security-as-a-service (SaaS) is a service delivery model for security management. Typically, Security as a Service involves applications such as anti-virus software delivered over the Internet but the term can also refer to security management provided in-house by an external organization.

Security Assertion Markup Language (SAML) – A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.

security association – A relationship established between two or more entities to enable them to protect data they exchange.

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

security audit – See audit.

security banner – A banner at the top or bottom of a computer screen that states the overall classification of the system in large, bold type. Also can refer to the opening screen that informs users of the security implications of accessing a computer resource.

Security Concept of Operations (Security CONOP) – A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system’s contribution to the operational mission.

Security Content Automation Protocol (SCAP) – A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

security control assessment – The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise.

security control baseline – The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

security control inheritance – A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See Common Control.

security controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

security engineering – An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

Security Fault Analysis (SFA) – An assessment usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.

Security Features Users Guide (SFUG) – Guide or manual explaining how the security mechanisms in a specific system work.

security impact analysis – The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

security incident – See incident.

security inspection – Examination of an information system to determine compliance with security policy, procedures, and practices. See audit

security perimeter – A physical or logical boundary that is defined for a system, domain, or enclave; within which particular security policy or security architecture is applied.

security policy – A set of criteria for the provision of security services.

security posture – The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

security relevant change – Any change to a system's configuration, environment, information content, functionality, or users which has the potential to change the risk imposed upon its continued operations.

security relevant event – An occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting).

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

security requirements baseline – Description of the minimum requirements necessary for an information system to maintain an acceptable level of risk.

Security Requirements Traceability Matrix (SRTM) – Matrix that captures all security requirements linked to potential risks and addresses all applicable C&A requirements. It is, therefore, a correlation statement of a system's security features and compliance methods for each security requirement.

security safeguards – Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Test and Evaluation (ST&E) – Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

sensitivity – A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

service level agreement – Defines the specific responsibilities of the service provider and sets the customer expectations.

signature – A recognizable, distinguishing pattern. See also attack signature or digital signature.

signature certificate – A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Simple Mail Transfer Protocol (SMTP) – The Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

situational awareness – Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

Six Sigma – A business management strategy, originally developed by Motorola in 1986. Six Sigma became well known after Jack Welch made it a central focus of his business strategy at General Electric in 1995, and today it is widely used in many sectors of industry and government.

Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction and/or profit increase).

smart card – A credit card-sized card with embedded integrated circuits that can store, process, and communicate information.

sniffer – See packet sniffer or passive wiretapping.

social engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used for identity theft or attacks against networks or computer systems.

software – Computer programs and associated data that may be dynamically written or modified during execution.

Software as a Service – The use of cloud computing to deliver software and associated data to clients Also referred to as "on-demand software"

software assurance – Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle and that the software functions in the intended manner.

software system test and evaluation – Process that plans, develops, and documents the qualitative/quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

solid state drive (SSD) – A data storage device that uses integrated circuit assemblies as memory to store data persistently. SSD technology uses electronic interfaces compatible with traditional block input/output (I/O) magnetic hard disk drives. SSDs do not employ any moving mechanical components, which distinguishes them from traditional magnetic disks such as hard disk drives (HDDs) or floppy disks, which are electromechanical devices containing spinning disks and movable read/write heads. Compared with electromechanical disks, SSDs are typically less susceptible to physical shock, are silent, lower power consumption, reduced heat signature and have lower access time and latency, but are currently more expensive per unit of storage than magnetic storage.

spam – Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

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

spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

steganography – The art, science, and practice of communicating in a way that hides the existence of the communication.

strong authentication – The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. See multi-factor authentication

SUDO – An operating system command that allows a general user to gain privileged access to an information system or application.

Supervisory Control and Data Acquisition (SCADA) – computer systems that monitor and control industrial, infrastructure, or facility-based processes, as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete tmodes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

(See also Industrial Control Systems.)

supply chain – A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

supply chain attack – Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

system – Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See also information system.

System Administrator (SA) – Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

System Development Life Cycle (SDLC) – The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System High Mode – Information systems security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: 1) valid security clearance for all information within an information system; 2) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments and/or special access programs); and 3) valid need-to- know for some of the information contained within the information system.

system integrity – Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

system interconnection – The direct connection of two or more information systems for the purpose of sharing data and other information resources.

System Security Plan (SSP) – The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

system-specific security control – A security control for an information system that has not been designated as a common control or the portion of a hybrid security control that is to be implemented within an information system.

super user – An individual granted a greater level of security access to an information system or application for the purposes of maintenance or support. (see privileged user)

survivability – In engineering, survivability is the quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance; e.g. nuclear electromagnetic pulse from the detonation of a nuclear weapon, tsunami, or Distributed Denial of Service attack (Ddos).

For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.

T

tampering – An intentional event resulting in modification of a system, its intended behavior, or data.

Target of Evaluation (TOE) – In accordance with Common Criteria, an information system, part of a system or product, and all associated documentation, that is the subject of a security evaluation.

Technical Reference Model (TRM) – A component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of service components and capabilities.

technical security controls – Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

technical vulnerability information – Detailed description of a weakness to include the implementable steps (such as code) necessary to exploit that weakness.

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

threat – 1) Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.;
2) An act with a negative consequence.

threat analysis – See threat assessment.

threat assessment – Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

threat monitoring – Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

threat source – The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally exploit vulnerability.

Theory of Constraints – Adopts the common idiom “A chain is no stronger than its weakest link” as a new management paradigm. This means that processes, organizations, etc., are vulnerable because the weakest person or part can always damage or break them or at least adversely affect the outcome.

The analytic approach with TOC comes from the contention that any manageable system is limited in achieving more of its goals by a very small number of constraints, and that there is always at least one constraint. Hence the TOC process seeks to identify the constraint and restructure the rest of the organization around it.

time bomb – Resident computer program that triggers an unauthorized act at a predefined time.

time-dependent password – Password that is valid only at a certain time of day or during a specified interval of time.

token – Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also cryptographic token.

Total Quality Management – A business management philosophy used by management for continuously improving the quality of output from manufacturing and business processes. (See also, 6 Sigma, Lean Six Sigma & Theory of Constraints.)

Traffic Analysis (TA) – Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow’s presence, amount, frequency, and duration of occurrence.

traffic padding – Generation of mock communications or data units to disguise the amount of real data units being sent.

Traffic-Flow Security (TFS) – Techniques by hackers, crackers or untrusted insiders to counter Traffic Analysis. (See also Anti-Forensics.)

tranquility – Property whereby the security level of an object cannot change while the object is being processed by an information system.

transmission – The state that exists when information is being electronically sent from one location to one or more other locations.

transmission security – Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

trap door – 1. A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data. (See also back door.)
2. In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information.

Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

trust list – The collection of trusted certificates used by relying parties to authenticate other certificates.

trusted agent – Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with Certification Authorities.

trusted certificate – A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."

trusted channel – A channel where the endpoints are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSL, IPSEC, and secure physical connection.

trusted computer system – A system that employs sufficient hardware and software assurance measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Computing Base (TCB) – Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

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

tunneling – Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Two-Person Control (TPC) – System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

Two-Person Integrity (TPI) – System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

U

unauthorized access – Any access that violates the stated security policy.

unauthorized disclosure – An event involving the exposure of information to entities not authorized access to the information.

untrusted process – Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

user – Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

user ID – Unique symbol or character string used by an information system or application to identify a specific user. Used in conjunction with a password or other authentication mechanism.

V

validation – Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).

verification – Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity’s attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome.

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

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

vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability assessment – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Assessment Review Team (VART) – Group of individuals assigned to review vulnerabilities, assess risks, make recommendations for mitigation and assist in patch management.

W

warm site – Backup site which typically contains the data links and pre-configured equipment necessary to rapidly start operations, but does not contain live data. Thus commencing operations at a warm site will (at a minimum) require the restoration of current data.

Web bug – Malicious code, invisible to a user, placed on web sites in such a way that it allows third parties to track use of web servers and collect information about the user, including IP address, host name, browser type and version, operating system name and version, and web browser cookie.

Wi-Fi Protected Access-2 (WPA-2) – The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For Federal government use, the implementation must use FIPS approved encryption, such as AES.

Wiki – Web applications or similar tools that allow identifiable users to add content (as in an Internet forum) and allow anyone to edit that content collectively.

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

Wireless Application Protocol (WAP) – A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

Wireless Equivalent Privacy (WEP) – A security algorithm for wireless networks. Introduced as part of the original wireless standard, its intention was to provide data confidentiality comparable to that of a traditional wired network. The algorithm uses key sizes of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favor of newer standards such as WPA2. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 “have been deprecated as they fail to meet their security goals”.

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

Work factor – Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See malicious code.

X, Y

X.509 Public Key Certificate – The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgettable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. Also known as X.509 Certificate.

Z

zero fill – To fill unused storage locations in an information system with the representation of the character denoting "0."

3. STATE OF HAWAI‘I EXECUTIVE BRANCH DEPARTMENTS, DIVISIONS, BRANCHES, OFFICES, BOARDS, COMMISSIONS & COUNCILS

Abbreviation	Definition	Department
AG	Department of Attorney General	
B&F	Department of Budget & Finance	
CIOC	Chief Information Officers Council	Governor
DAGS	Department of Accounting and General Services	
DBEDT	Department of Business Economic Development & Tourism	
DHHL	Department of Hawaiian Home Lands	
DHRD	Department of Human Resources	
DLIR	Department of Labor & Industrial Relations	
DLNR	Department of Land and Natural Resources	
DOA	Department of Agriculture	
DOE	Department of Education	
DOH	Department of Health	
DOT	Department of Transportation	
DOTAX	Department of Taxation	
ELC	Executive Leadership Council	Governor
HCJDS	Hawai‘i Criminal Justice Data Center	AG
HDOD	Hawai‘i Department of Defense	
HPA	Hawai‘i Paroling Authority	PSD
ICSD	Information & Communications Services Division	DAGS
IPSC	Information Privacy & Security Council	DAGS
JJIS	Juvenile Justice Information Services	AG
OIMT	Office of Information Management and Technology	DAGS
PSD	Public Safety Department	
SCD	State Civil Defense	HDOD
SOH	State of Hawai‘i	
SSB	System Services Branch	ICSD
SPO	State Procurement Office	DAGS
TSSB	Telecommunication Shared Services Branch	ICSD
UH	University of Hawai‘i	

4. CIO COUNCIL ADVISORY WORKING GROUPS

Governance & Policy	Technology	Shared Services
Enterprise Architecture (EA)	Networks	Enterprise Resource Planning (ERP)
Policy	Computing and Storage	Global Information Systems (GIS)
People & Organization	Information Assurance & Privacy	Records Management
Innovation	Operations	Email & Collaboration
IT Procurement	Development	

5. COMMONLY USED TECHNICAL ABBREVIATIONS AND ACRONYMS

Acronym	Definition
(ISC)2®	International Information Systems Security Certification Consortium, Inc.
3G	3rd Generation
4G	4th Generation
6∑	6 SIGMA
APT	Advanced Persistent Threat
BPR	Business Process Reengineering
C&A	Configuration & Accreditation
CCB	Change Control Board
CCNA	Cisco Certified Network Associate
CCNE	Cisco Certified Network Engineer
CCSP	Cisco Certified Security Professional
CEH	Certified Ethical Hacker
CIA	Confidentiality Integrity Availability
CIO	Chief Information Officer
CIOC	Chief Information Officer Council
CIP	Capital Infrastructure Planning
CISO	Chief Information Security Officer
CISSP	Certified Information Security Services Professional
COE	Center of Excellence
CSTCB	Cyber Security Technology & Controls Branch
CS	Cyber Security
CSIRT	Computer Security Incident Response Team
CTA	Chief Technical Architect
DAM	Database Access Management
DAR	Data at Rest
DC	Data Center
DCIO	Deputy Chief Information Officer
DIACAP	Defense Information Assurance Certification and Accreditation Program

Acronym	Definition
DIM	Data in Motion
DLP	Data Loss Prevention
DISO	Department Information Security Officer
EA	Enterprise Architecture
ELC	Enterprise Leadership Council
ERP	Enterprise Resource Management
FEDRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information System Management Act
FTE	Full Time Equivalent
FTP	File Transfer Protocol
GLB	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HRM	Human Resource Management
HWIN	Hawai‘i Wireless Interoperability Network
IA	Information Assurance
IaaS	Infrastructure as a Service
IACSD	Information Assurance & Cyber Security Division
IAMSG	Identity & Access Management/Security Governance
ICAM	Identity
ICS	Industrial Control System
IRM	Information Resource Management
IS	Information System / Information Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMR	Land Mobile Radio
LTE	Long Term Evolution
MAN	Metropolitan Area Network
MOA	Memo of Agreement
MOU	Memorandum of Understanding
NGN	Next Generation Network
NIST	National Institute for Standards and Technology
NOC	Network Operations Center
OIMT	Office of Information Management & Technology

Acronym	Definition
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry – Data Security Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Program Management
POA&M	Plan of Action & Milestones
RFC	Request for Change
RPZ	Regional Planning Zone
RTM	Requirements Traceability Matrix
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SecSaaS	Security as a Service
SCIP	Statewide Communications Interoperability Plan
SIGB	Statewide Interoperability Governing Body
SOC	Security Operations Center
SOCB	Security Operations Branch
SOX	Sarbanes Oxley Act
SSD	Solid State Drive
SSO	Single Sign On
TA	Traffic Analysis
TCB	Trusted Computing Base
TFS	Traffic-Flow Security
TOC	Theory of Constraints
TPI	Two-Person Integrity
TQM	Total Quality Management
VART	Vulnerability Assessment and Review Team
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point / Wireless Application Protocol
WEP	Wireless Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA-2	Wi-Fi Protected Access II
VPN	Virtual Private Network

NOTES

NOTES

NOTES

NOTES

REFERENCES

The following documents were used in whole or in part as background material in development of this policy:

1. Public Law 107-347 [H.R. 2458], The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002, December 2002.

2. CNSSI No. 4016, National Information Assurance Training Standard for Risk Analysts, November 2005.

3. Public Law 104-106, Clinger-Cohen Act of 1996, January 1996.

4. Committee on National Security Systems Instruction (CNSSI) No. 4009, National Information Assurance Glossary.

5. Public Law 108-458, Intelligence Reform and Terrorism Act of 2004, December 2004.

6. Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001.

7. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 2005.

8. Office of Management and Budget Transmittal Memorandum No. 4, Circular A-130, Management of Federal Information Resources, November 2000.

9. Federal Information Processing Standard Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

10. Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

11. CNSS Policy No. 6, National Policy on Certification and Accreditation of National Security Systems, October 2005.

12. CNSS Directive No. 502, National Directive on Security of National Security Systems, December 2004.

13. DoD Instruction 8500.2, Information Assurance Implementation, February 2003.

14. CNSSI No. 4014, Information Systems Security Officers National Information Assurance Training Standard, March 2004