IAPP Governmental Privacy Certification

Glossary of Public Sector Privacy Terminology

Acceptable Risk

"A concern that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures." *(Source: NIST SP 800-18 and SP 800-26).*

Accreditation

See also: *Authorize Processing, Certification and Accreditation* and *Designated Approving Authority*

"Synonymous with the term authorize processing. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security." *(Source: NIST SP 800-18).*

Access

"The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource." (This definition applies to "access" as used in this subpart, not as used in subpart E of this part.) *(Source: HIPAA Regulations).*

Access Controls

Tools used to limit unauthorized access to a system. These include user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. *(Source: NIST SP 800-18).*

Administrative safeguards

"Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." *(Source: HIPAA Regulations).*

Adverse Action

"(i) [A] denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance;

(ii) a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee; (iii) a denial or cancellation of, an increase in any charge for, or any other adverse or unfavorable change in the terms of, any license or benefit described in section 604(a)(3)(D) [§ 1681b]; and (iv) an action taken or determination that is (I) made in connection with an application that was made by, or a transaction that was initiated by, any consumer, or in connection with a review of an account under section 604(a)(3)(F)(ii)[§ 1681b]; and (II) adverse to the interests of the consumer. (2) Applicable findings, decisions, commentary, and orders. For purposes of any determination of whether an action is an adverse action under paragraph (1)(A), all appropriate final findings, decisions, commentary, and orders issued under section 701(d)(6) of the Equal Credit Opportunity Act by the Board of Governors of the Federal Reserve System or any court shall apply." *(Source: FCRA).*

Agency

"Any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." *(Source: FOIA)*; "[A]ny executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration." *(Source: OMB A-130)*

Aggrieved Person

"A person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." *(Source: ECPA).*

Affiliate

"Any company that controls, is controlled by, or is under common control with another company." *(Source: GLB).*

Anonymization of Data

"[R]efers to techniques used to allow data to be shared or searched without disclosing identity." (Source: http://www.heritage.org/Research/HomelandDefense/lm11.cfm).

Application

"Any data entry, update, query, or report program that processes data for the user. It includes not only the generic productivity software (spreadsheets, word processors, database programs, etc.) but also custom and packaged programs for payroll, billing, inventory, and other accounting purposes." *(Source: NIST SP 800-40).* As necessary to effect, administer, or enforce the transaction' – "(A) the disclosure is required, or is a usual, appropriate, or acceptable method, to carry out the transaction or the product or service business of which the transaction is a part, and record or service or maintain the consumer's account in the ordinary course of providing the financial service or financial product, or to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part, and includes - (i) providing the consumer or the consumer's agent or broker with a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product; and (ii) the accrual or recognition of incentives or bonuses associated with the transaction that are provided by the financial institution or any other party; (B) the disclosure is required, or is one of the lawful or appropriate methods, to enforce the rights of the financial institution or of other persons engaged in carrying out the financial transaction, or providing the product or service; (C) the disclosure is required, or is a usual, appropriate, or acceptable method, for insurance underwriting at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: Account administration, reporting, investigating, or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance

benefits (including utilization review activities), participating in research projects, or as otherwise required or specifically permitted by Federal or State law; or (D) the disclosure is required, or is a usual, appropriate or acceptable method, in connection with - (i) the authorization, settlement, billing, processing, clearing, transferring, reconciling, or collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment card, check, or account number, or by other payment means; (ii) the transfer of receivables, accounts or interests therein; or (iii) the audit of debit, credit or other payment information." *(Source: GLB).*

Asset

"A major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems." *(Source: NIST SP 800-26)*; "Information resources that support an organization's mission." *(Source: NIST SP 800-12).*

Audit Trail

"[A]record showing who has accessed an IT system and what operations the user has performed during a given period." *(Source: NIST SP 800-47).*

Aural Transfer

"[A] transfer containing the human voice at any point between and including the point of origin and the point of reception. *(Source: ECPA)*

Authentication

"The broadest definition of authentication within computing systems encompasses identity verification, message origin authentication, and message content authentication." *(Source: NIST SP 800-21);* "The process of verifying the authorization of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system." *(Source: NIST SP 800-47).*

Authority to Process Information

See also: *Designated Approving Authority*

"Occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it." *(Source: NIST SP 800-18).*

Automated Key Distribution

"The distribution of cryptographic keys, usually in encrypted form, using electronic means, such as a computer network." *(Source: NIST SP 800-21).*

Awareness, Training and Education

"Includes (1) awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security." *(Source: NIST SP 800-18).*

Availability

"The property that data or information is accessible and useable upon demand by an authorized person." *(Source: HIPAA Regulations).*

Binding

"An acknowledgment by a trusted third party that associates an entity's identity with its public key. This may take place through (1) a certification authority's generation of a public key certificate, (2) a security officer's verification of an entity's credentials and placement of the entity's public key and identifier in a secure database, or (3) an analogous method." *(Source: NIST SP 800-21).*

Business Associate (HIPAA)

Capital planning and investment control process – "[A] management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes." *(Source: OMB A-130).*

Certificate (or public key certificate)

"A digitally signed data structure defined in the X.509 standard that binds the identity of a certificate holder (or subject) to a public key." *(Source: NIST SP 800-21).*

Certificate Revocation List (CRL)

"[A] list of revoked but unexpired certificates issued by a Certification Authority." *(Source: NIST SP 800-21).*

Certification

See also: *Accreditation, Authority to Process Information, Designated Approving Authority*,

A term that is "synonymous with the term authorize processing. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements." *(Source: NIST SP 800-18)*; "Certification involves the testing and evaluation of the technical and non-technical security features of an IT system to determine its compliance with a set of specified security requirements. Accreditation is a process whereby a Designated Approval Authority (DAA) or other authorizing management official authorizes an IT system to operate for a specific purpose using a defined set of safeguards at an acceptable level of risk." *(Source: NIST SP 800-47).*

Certification Authority

"A trusted entity that issues certificates to end entities and other Certification Authorities (CA). CAs issue Certificate Revocation Lists (CRL) periodically, and post certificates and CRLs to a repository." *(Source: NIST SP 800-21).*

Certification Path

"An ordered sequence of certificates, leading from a certificate whose public key is known by a client, to a certificate whose public key is to be validated by the client." *(Source: NIST SP 800-21).*

Chief Information Officer (CIO)

"Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency." *(Source: Clinger-Cohen).*

Child

"[A]n individual under the age of 13." *(Source: COPPA).*

Ciphertext

"Encrypted (enciphered) data." *(Source: NIST SP 800-21*).

Claimant

"An entity which is or represents a principal for the purposes of authentication, together with the functions involved in an authentication exchange on behalf of that entity. A claimant acting on behalf of a principal must include the functions necessary for engaging in an authentication exchange (e.g., a smartcard (claimant) can act on behalf of a human user (principal))." *(Source: NIST SP 800-21).*

Classified Information

"Classified information or classified national security information means information that has been determined pursuant to E. O. 12958 as amended by E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form." *(Source: NIST SP 800-59).*

Cold Site

"A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site." *(Source: NIST SP 800-34).*

Collection of Information

"[A] means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either— (i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or (ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and (B) shall not include a collection of information described under section 3518 (c)(1)." *(Source: Paperwork Reduction Act).*

Communication Common Carrier

"Has the meaning given that term in section 3 of the Communications Act of 1934." *(Source: ECPA)*

Compromise

"The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other critical security parameters)." *(Source: NIST SP 800-21).*

Computer Matching

Computer Trespasser – "(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." *(Source: ECPA).*

Confidentiality

A process by which "sensitive information is not disclosed to unauthorized individuals, entities or processes." *(Source: NIST SP 800-21)*; "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." *(44 U.S.C. Sec. 3542)*; "[T]he property that data or information is not made available or disclosed to unauthorized persons or processes." *(Source: HIPAA Regulations)*.

Confidentiality Protection

"Requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress." *(Source: NIST SP 800-18)*.

Consumer

"An individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." (Source: GLB); "[A]n individual." *(Source: FCRA)*.

Consumer Report

"Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [§ 1681b]. (2) Exclusions. The term "consumer report" does not include: (A) any (i) report containing information solely as to transactions or experiences between the consumer and the person making the report; (ii) communication of that information among persons related by common ownership or affiliated by corporate control; or (iii) communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons; (B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device; (C) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the disclosures to the consumer required under section 615 [§ 1681m]; or (D) a communication described in subsection (o). *(Source: FCRA)*.

Consumer Reporting Agency

"Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." *(Source: FCRA)*.

Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis

"[A] consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide: (1) Public record information. (2) Credit account information from persons who furnish that information regularly and in the ordinary course of business." *(Source: FCRA)*.

Contents

"When used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. *(Source: ECPA)*

Counterintelligence

"The term 'counterintelligence' means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." *(Source: NIST SP 800-59).*

Contingency Plan

"Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster." *(Source: NIST SP 800-34).*

Continuity of Operations Plan (COOP)

"A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations." *(Source: NIST SP 800-34*).

Covered Entity (HIPAA)

"(1) A health plan; (2) A health care clearinghouse; (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." (Source: HIPAA Regulations). "Credit or insurance transaction that is not initiated by the consumer" – "[D]oes not include the use of a consumer report by a person with which the consumer has an account or insurance policy, for purposes of (1) reviewing the account or insurance policy; or (2) collecting the account. *(Source: FCRA).*

Cryptographic Key

A parameter used in conjunction with a cryptographic algorithm that determines: (1) the transformation of plaintext data into ciphertext data, (2) the transformation of ciphertext data into plaintext data, (3) a digital signature computed from data, (4) the verification of a digital signature computed from data, or (5) a data authentication code (DAC) computed from data. *(Source: NIST SP 800-21).*

Cryptography

"The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof." "Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption." *(Source: NIST SP 800-21).*

Customer

"[A]ny person or authorized representative of that person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary, in relation to an account maintained in the person's name

Data Element

"A basic unit of information that has a unique meaning and subcategories (data items) of distinct value. Examples of data elements include gender, race, and geographic location." *(Source: NIST SP 800-47).*

Data Integrity

See also: *Integrity*

"The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction." *(Source: NIST SP 800-21).*

Data Aggregation

"With respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities." *(Source: HIPAA Regulations)*

Data Augmentation

Obtaining information from other sources, such as commercial databases, to add to information that is already in an entity's database.

Data-mining

"[T]he application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results." *(Source: GAO Report, Data Mining: Federal Efforts Cover Wide Range of Uses, May 2004. http://www.gao.gov/new.items/d04548.pdf).*

Data Surveillance ("Dataveillance")

"[A] surveillance of large groups of people – to sift through vast amounts of personally identifying data to find individuals who might fit a terrorist profile." *(Source: GAO Report, Data Mining: Federal Efforts Cover Wide Range of Uses, May 2004. http://www.gao.gov/new.items/d04548.pdf).*

Data Trail

A collection of information that reveals the places where an individual has actually been or things he has done.

Data Warehouse

Dates of Attendance – "[T]he period of time during which a student attends or attended an educational agency or institution. Examples of dates of attendance include an academic year, a spring semester, or a first quarter… The term does not include specific daily records of a student's attendance at an educational agency or institution." *(Source: FERPA).*

Decryption

"The process of changing ciphertext into plaintext." *(Source: NIST SP 800-21).*

Derived Data

Designated Record Set (HIPAA) – "(1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes

protected health information and is maintained, collected, used, or disseminated by or for a covered entity." *(Source: HIPAA Regulations)*

Designated Approving Authority

"The senior management official who has the authority to authorize processing (accredit) an automated information (major application) or (general support system) and accept the risk associated with the system." *(Source: NIST SP 800-18).*

Digital Signature

The result of a cryptographic transformation of data which, when properly implemented, provides the services of: (1) origin authentication, (2) data integrity, and (3) signer non-repudiation. The digital signature is computed using a set of rules (e.g., the Digital Signature Algorithm (DSA)) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. [. . .]. A data unit that allows a recipient of a message to verify the identity of the signatory and integrity of the message. [. . .]. A nonforgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data." *(Source: NIST SP 800-21).*

Directory Information

"Information contained in an education record of a student which would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended." *(Source: FERPA Regulations).*

Direct treatment relationship

"[A] treatment relationship between an individual and a health care provider that is not an indirect treatment relationship." *(Source: HIPAA Regulations)*

Disclosure

"To permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." (Source: FERPA Regulations); "[T]he release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information." *(Source: HIPAA Regulations);* "[W]ith respect to personal information— (A) the release of personal information collected from a child in identifiable form by an operator for any purpose, except where such information is provided to a person other than the operator who provides support for the internal operations of the website and does not disclose or use that information for any other purpose; and (B) making personal information collected from a child by a website or online service directed to children or with actual knowledge that such information was collected from a child, publicly available in identifiable form, by any means including by a public posting, through the Internet, or through— (i) a home page of a website; (ii) a pen pal service;(iii) an electronic mail service; (iv) a message board; or (v) a chat room." *(Source: COPPA).*

Disciplinary Action or Proceeding

" The investigation, adjudication, or imposition of sanctions by an educational agency or institution with respect to an infraction or violation of the internal rules of conduct applicable to students of the agency or institution." *(Source: FERPA Regulations).*

Dissemination

The government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act. *(Source: OMB A-130)*

Drivers Privacy Protection Act

Generally prohibits state Departments of Motor Vehicles from disclosing personal information submitted by individuals in order to obtain driver's licenses. The Act requires that states disclose personal information for certain purposes and allows disclosure for certain enumerated purposes. In 2000, the Act was amended by creating ca new class of "highly restricted personal information." Highly restricted personal information includes an individual's photograph or image, social security number, and medical or disability information. This information may not be shared without the express consent of the person to whom the information applies, except for four enumerated purposes stated in the Act.

Educational Agency or Institution

"Any public or private agency or institution which is the recipient of funds under any applicable program." *(Source: FERPA*)

Education Records (FERPA)

Those records, files, documents, and other materials which: contain information directly related to a student; and are maintained by an educational agency or institution or by a person acting for such agency or institution. The term "education records" does not include: records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute; records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement; in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice. *(Source: FERPA)*

Electronic Communication

"Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce, but does not include: (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds. *(Source: ECPA)*

Electronic Communications Service

"Any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *(Source: ECPA).*

Electronic Communications System

"Any service which provides to users thereof the ability to send or receive wire or electronic communications. *(Source: ECPA).*

E-Government Act of 2002

See also: *Privacy Impact Assessment, Information Technology*

A federal law that, among other things, requires federal agencies to conduct Privacy Impact Assessments on new or substantially revised information technology.

Electronic, Mechanical or Other Device

"Any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than— (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties**;** (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal. *(Source: ECPA)*

Electronic Signature

"A method of signing an electronic message that -- (A) Identifies and authenticates a particular person as the source of the electronic message; and Implementing Cryptography 123 (B) Indicates such person's approval of the information contained in the electronic message. [GPEA]." *(Source: NIST SP 800-21).*

Electronic Storage

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *(Source: ECPA)*

Employment Purposes

"When used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee." *(Source: FCRA)*

Encrypted Key (Ciphertext Key)

"A cryptographic key that has been encrypted with a key encrypting key, a PIN or a password to disguise the value of the underlying plaintext key." *(Source: NIST SP 800-21).*

Encryption

"The process of changing plaintext into ciphertext for the purpose of security or privacy." *(Source: NIST SP 800-21)*; "The translation of data into a form that is unintelligible without a deciphering mechanism. *(Source: NIST SP 800-47)*; "The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *(Source: HIPAA Regulations)*

Enterprise Architecture

``(i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (B) includes-- (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan." *(Source: E-Gov Act)*

Excluded Communications

A communication: "(1) that, but for subsection (d)(2)(D) [of FCRA], would be an investigative consumer report; (2) that is made to a prospective employer for the purpose of (A) procuring an employee for the employer; or (B) procuring an opportunity for a natural person to work for the employer; (3) that is made by a person who regularly performs such procurement; (4) that is not used by any person for any purpose other than a purpose described in subparagraph (A) or (B) of paragraph (2); and (5) with respect to which (A) the consumer who is the subject of the communication (i) consents orally or in writing to the nature and scope of the communication, before the collection of any information for the purpose of making the communication; (ii) consents orally or in writing to the making of the communication to a prospective employer, before the making of the communication; and (iii) in the case of consent under clause (i) or (ii) given orally, is provided written confirmation of that consent by the person making the communication, not later than 3 business days after the receipt of the consent by that person; (B) the person who makes the communication does not, for the purpose of making the communication, make any inquiry that if made by a prospective employer of the consumer who is the subject of the communication would violate any applicable Federal or State equal employment opportunity law or regulation; and (C) the person who makes the communication (i) discloses in writing to the consumer who is the subject of the communication, not later than 5 business days after receiving any request from the consumer for such disclosure, the nature and substance of all information in the consumer's file at the time of the request, except that the sources of any information that is acquired solely for use in making the communication and is actually used for no other purpose, need not be disclosed other than under appropriate discovery procedures in any court of competent jurisdiction in which an action is brought; and (ii) notifies the consumer who is the subject of the communication, in writing, of the consumer's right to request the information described in clause (i). *(Source: FCRA).*

False Positives

Database query results that flag a pattern as being terrorist-related when it is not**.**

False Negatives

Database query that fails to flag a pattern as being terrorist related when it actually is terrorism related.

Federal Benefit Program

"Any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals." *(Source: Privacy Act).*

Federal Functional Regulator

"(A) the Board of Governors of the Federal Reserve System; (B) the Office of the Comptroller of the Currency; (C) the Board of Directors of the Federal Deposit Insurance Corporation; (D) the Director of the Office of Thrift Supervision; (E) the National Credit Union Administration Board; and (F) the Securities and Exchange Commission." *(Source: GLBA).*

Federal Information System

"An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency." *(Source: NIST SP 800-59).*

Federal Personnel

"Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits)." *(Source: Privacy Act).*

File

"When used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored." *(Source: FCRA).*

Financial Institution

Any institution the business which is engaging in financial activities as described in section 1843(k) of title 12. *(Source: GLB).* The term "financial institution" does not include: (1) any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.); (2) the Federal Agricultural Mortgage Corporation; or (3) any entity chartered and operating under the Farm Credit Act of or institutions chartered by Congress specifically to engage in transactions described in section 6802(e)(1)(C) of this title, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party. *(Source: GLB)*; "[A]ny office of a bank, savings bank, card issuer as defined in section 1602 (n) of title 15, industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands." *(Source: Right to Financial Privacy Act).*

Financial Record

"An original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution." *(Source: Right to Financial Privacy Act).*

Firewall

"A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both." *(Source: NIST SP 800-47).*

Firm offer of credit or insurance

"Any offer of credit or insurance to a consumer that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer, except that the offer may be further conditioned on one or more of the following: (1) The consumer being determined, based on information in the consumer's application for the credit or insurance, to meet specific criteria bearing on credit worthiness or insurability, as applicable, that are established (A) before selection of the consumer for the offer; and (B) for the purpose of determining whether to extend credit or insurance pursuant to the offer. (2) Verification (A) that the consumer continues to meet the specific criteria used to select the consumer for the offer, by using information in a consumer report on the consumer, information in the consumer's application for the credit or insurance, or other information bearing on the credit worthiness or insurability of the consumer; or (B) of the information in the consumer's application for the credit or insurance, to determine that the consumer meets the specific criteria bearing on credit worthiness or insurability. (3) The consumer furnishing any collateral that is a requirement for the extension of the credit or insurance that was (A) established before selection of the consumer for the offer of credit or insurance; and (B) disclosed to the consumer in the offer of credit or insurance." *(Source: FCRA).*

Foreign Intelligence Information

"[F]or purposes of section 2517 (6) [of the ECPA], means: **(A)** information, whether or not concerning a United States person, that relates to the ability of the United States to protect against: **(i)** actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; **(ii)** sabotage or international terrorism by a foreign power or an agent of a foreign power; or **(iii)** clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or **(B)** information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to— (i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States." *(Source: ECPA).*

General Exemptions

Rules promulgated by the head of any agency to exempt any system of records within the agency from certain specific requirements in the Privacy Act. *(Source: the Privacy Act).*

General Support System

"[A]n interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations." (Source: NIST SP 800-18). Government Information – "[I]nformation created, collected, processed, disseminated, or disposed of by or for the Federal Government." *(Source: OMB A-130).*

Government Publication

"[I]nformation which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)." *(Source: OMB A-130).*

Group Health Plan

"[A]n employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that: (1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or (2) Is administered by an entity other than the employer that established and maintains the plan." *(Source: HIPAA Regulations).*

Health Care

"[C]are, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription." *(Source: HIPAA Regulations).*

Health Care Clearinghouse

"[A] public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard

transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity." *(Source: HIPAA Regulations).*

Health Care Operations

"[A]ny of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates: (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable; (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and (6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances; (iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and (v) Consistent with the applicable requirements of § 164.514, creating de- identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2) *(Source: HIPAA Regulations).*

Health Care Provider

"[A] provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. *(Source: HIPAA Regulations)*

Health Information

Any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. *(Source: HIPAA Regulations).*

Health insurance issuer

"(as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is

licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan." *(Source: HIPAA Regulations).*

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Title I of HIPAA protects employees' health insurance coverage when they leave their jobs. Title II provides standards for patient health, administrative and financial data interchange. Title II also addresses the requirements for the privacy and security of health information records and transactions. HIPAA became law in 2001, but compliance was required in phases up until 2004.

Health maintenance organization (HMO)

"([A]s defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO." *(Source: HIPAA Regulations).*

Health Oversight Agency

"[A]n agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant." *(Source: HIPAA Regulations).*

Health Plan

"[A]n individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)). (1) Health plan includes the following, singly or in combination: (i) A group health plan, as defined in this section. (ii) A health insurance issuer, as defined in this section. (iii) An HMO, as defined in this section. (iv) Part A or Part B of the Medicare program under title XVIII of the Act. (v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq. (vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)). (vii) An issuer of a long-term care policy, excluding a nursing home fixed- indemnity policy. (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. (ix) The health care program for active military personnel under title 10 of the United States Code. (x) The veterans health care program under 38 U.S.C. chapter 17. (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)). (xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq. (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq. (xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq. (xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28. (xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals. (xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). (2) Health plan excludes: (i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (ii) A government-funded program (other than one listed in paragraph (1)(i)- (xvi)of this definition): (A) Whose principal purpose is other than providing, or paying the cost of, health care; or (B) Whose principal activity is: (1) The direct provision of health care to persons; or (2) The making of grants to fund the direct provision of health care to persons." *(Source: HIPAA Regulations).*

Holding Company

"(A) any bank holding company (as defined in section 1841 of this title); (B) any company described in section 1843 (f)(1) of this title; and (C) any savings and loan holding company (as defined in the Home Owners' Loan Act [12 U.S.C. 1461 et seq.])." *(Source: RFPA).*

Hot Site

"A fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster." *(Source: NIST SP 800-34).*

Identifiable Form

"[A]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." *(Source: E-Government Act).*

Identification

"The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system." *(Source: NIST SP 800-47).*

Immutable Audits

"Audit trails that cannot be disabled or changed. Immutable Audits ensure that (1) "everyone is subject to an audit"; (2) "produce cross-organizational audits"; (3) "measure accuracy of auditors by cross-validation;" and (4) "produce user logs that are tamper resistant." *(Source: http://www.heritage.org/Research/HomelandDefense/lm11.cfm).*

Indirect Treatment Relationship

"[A] relationship between an individual and a health care provider in which: (1) The health care provider delivers health care to the individual based on the orders of another health care provider; and (2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual." *(Source: HIPAA Regulations)*

Individual

"[A] citizen of the United States or an alien lawfully admitted for permanent residence." *(Sources: Privacy Act and the OMB PIA Guidance);* "[T]he person who is the subject of protected health information." *(Source: HIPAA Regulations)*

Individual Accountability

"Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules." *(Source: NIST SP 800-26).*
Individually Identifiable Health Information – "[I]nformation that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual." (Source: HIPAA Regulations)
Information – "[A]ny communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms." *(Source: OMB A-130).*
Information Dissemination Product - "[A]ny book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public." *(Source: OMB A-130).*

Information in Identifiable Form

"Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)." (*OMB PIA Guidance).*

Information Life Cycle

"The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition." *(Source: OMB A-130).*

Information Owner

"Is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations." *(Source: NIST SP 800-26).*

Information Processing Services Organization (IPSO)

"A discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis." *(Source: OMB A-130).*

Information Management

"The planning, budgeting, manipulating, and controlling of information throughout its life cycle." *(Source: OMB A-130)*

Information Resources

"Information and related resources, such as personnel, equipment, funds, and information technology." (Source: NIST SP 800-59 and the Paperwork Reduction Act); "[I]ncludes both government information and information technology." *(Source: OMB A-130)*

Information Resources Management

"The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology." *(Source: OMB A-130 and the Paperwork Reduction Act).*

Information Security

"Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability." *(Source: NIST SP 800-59).*

Information System

"A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual." *(Source: OMB A-130)*; "[A] discrete set of information [44 USC 3502 (8)] resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." *(Source: NIST SP 800-59);* "[A]n interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people." *(Source: HIPAA Regulations)*

Information System Life Cycle

"[T]he phases through which an information system passes, typically characterized as initiation, development, operation, and termination." *(Source: OMB A-130).*

Information Technology

"[A]ny equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information." *(Source: OMB PIA Guidance);* "[A]ny 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 an 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 (i) requires the use of such equipment, or (ii) 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. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452)." *(Source: OMB A-130 and Clinger-Cohen)*

Institution of Postsecondary Education

"[A]n institution that provides education to students beyond the secondary school level; "secondary school level" means the educational level (not beyond grade 12) at which secondary education is provided as determined under State law." *(Source: FERPA Regulations).*

Integrity

See also: *Data Integrity.*

"The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. . . . Integrity refers to assurance that a message was not modified accidentally or deliberately in transit, by replacement, insertion or deletion." *(Source: NIST SP 800-21)*; "The property that data or information have not been altered or destroyed in an unauthorized manner." *(Source: HIPAA Regulations)*

Intelligence

"(1) the product resulting from the [. . .] collection, processing, integration, analysis, evaluation, and [50 USC Ch 15] interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence." *(Source: NIST SP 800-59).*

Intelligence Activities

"The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities."

Intercept

"[T]he aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *(Source: ECPA)*

Interconnection Security Agreement (ISA)

"In this guide, an agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/A) between the organizations." *(Source: NIST SP 800-47).*

Internet

"[C]ollectively[,] the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/ Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio." *(Source: COPPA).*

Intrusion Detection System (IDS)

"A software application that can be implemented on host operating systems or as network devices to monitor activity that is associated with intrusions or insider misuse, or both." *(Source: NIST SP 800-47);* "[A] software application that can be implemented on host operating systems or as network devices to monitor for signs of intruder activity and attacks." *(Source: NIST SP 800-41).*

Investigative Consumer Report

"[A] consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer." *(Source: FCRA)*

Investigative or Law Enforcement Officer

"[A]ny officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses." *(Source: ECPA)*

Joint Agreement

"A formal written contract pursuant to which two or more financial institutions jointly offer, endorse, or sponsor a financial product or service, and as may be further defined in the regulations prescribed under section 6804 of this title." *(Source: GLB).*

Key Encrypting Key

"A cryptographic key that is used for the encryption or decryption of other keys." *(Source: NIST SP 800-21).*

Key Management

"The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, counters) during the entire life cycle of the keys, including the generation, storage, distribution, entry and use, deletion or destruction, and archiving. [. . .] The generation, storage, secure distribution and application of keying material in accordance with a security policy that prevents its modification, unauthorized use, or a combination thereof." *(Source: NIST SP 800-21).*

Knowledge Discovery and Data Mining (KDDM)

"[A]n "umbrella term describing several activities and techniques for extracting information from data and suggesting patterns in very large databases." *(Source: http://www.cit.gu.edu.au/~s2130677/teaching/KDD.d/readings.d/AICE99.pdf).*

Law Enforcement Inquiry

"[A] lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant thereto." *(Source: RFPA).*

Maintain

"Includes maintain, collect, use or disseminate." *(Source: Privacy Act).*

Major Application

"[A]n application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function." (Source: NIST SP 800-18); Major Information System - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources." *(Source: OMB PIA Guidance).*

Marketing

"[T]o make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. (1) Marketing does not include communications that meet the requirements of paragraph (2) of this definition and that are made by a covered entity: (i) For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or (ii) That are tailored to the circumstances of a particular individual and the communications are: (A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or (B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care. (2) A communication described in paragraph (1) of this definition is not included in marketing if: (i) The communication is made orally; or (ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication." *(Source: HIPAA Regulations)*

Mass Data-veillance

Using personal information contained in multiple sources to investigate or monitor the communications or activities of groups of individuals.

Matching Program (from The Privacy Act of 1974)

"Any computerized comparison of two or more automated systems of records or a system of records with non-Federal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with

respect to, cash or in-kind assistance or payments under Federal benefit programs, or recouping payments or delinquent debts under such Federal benefit programs, or two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records. The term does not include: (1) matches performed to produce aggregate statistical data without any personal identifiers; (2) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals; (3) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons; (4) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act; (5) matches using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or conducted by an agency using only records from systems of records maintained by that agency if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel; (6) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel; (7) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or (8) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. § 402(x)(3), § 1382(e)(1)." *(Source: The Privacy Act of 1074).*

Material Weakness or significant weakness

A term "used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. 'Material weakness' is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management." *(Source: NIST SP 800-26).*

Medical Information

"[I]nformation or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities." *(Source: FCRA)*

Memorandum of Understanding/Agreement (MOU/A)

"A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide [NIST SP 800-47], an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection." *(Source: NIST SP 800-47).*

Mission Creep (aka "Task Accretion" and "Mission Leap")

Generally involves the collection of personal information for a particular purpose and subsequently discovering additional, secondary uses to which the information can be put.

Mission Critical System

"[A]ny telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that: (A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or(C) processes any information, the loss, misuse,

disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency." *(Source:).*

Motor Vehicle Record

"[A]ny record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." *(Source: Drivers Privacy Protection Act).*

National Security Systems

"As defined in the Clinger-Cohen Act[4], an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management." (Sources: OMB PIA Guidance and the Clinger-Cohen Act); "[A]ny telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations." (44 U.S.C. 2901(2))." *(Source: OMB A-130).*

Networks

"Include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet." *(Source: NIST SP 800-18).*

Nonaffiliated Third Party (GLBA)

"Any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution." *(Source: GLB)*

Non-Federal Agency

"Any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program." *(Source: Privacy Act of 1974)*

Nonpublic Personal Information

"Personally identifiable financial information - (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. The term personally identifiable financial information does not include publicly available information, as such term is defined by the regulations prescribed under section 6804 of GLB. The term also shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information. The term shall include, however, any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information." *(Source: GLB)*

Non-repudiation

"This service provides proof of the integrity and origin of data that can be verified by a third party. [. . .] Non-repudiation of origin is protection against a sender of a message later denying transmission." *(Source: NIST SP 800-21).*

Office of Information and Regulatory Affairs

"Is a Federal office that Congress established in the 1980 Paperwork Reduction Act. OIRA is an office within the Office of Management and Budget, which is an agency within the Executive Office of the President. [. . .] In addition to reviewing draft regulations under Executive Order 12866, OIRA reviews collections of information under the Paperwork Reduction Act, and also develops and oversees the implementation of government-wide policies in the areas of information technology, information policy, privacy, and statistical policy." *(Source: http://www.whitehouse.gov/omb/inforeg/qa_2-25-02.pdf).*

Online Contact Information

"An e-mail address or an-other substantially similar identifier that permits direct contact with a person online." *(Source: COPPA).*

Operational Controls

"Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems)." *(Source: NIST SP 800-18).*

Operator

"Any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce— (i) among the several States or with 1 or more foreign nations; (ii) in any territory of the United States or in the District of Columbia, or between any such territory and— (I) another such territory; or (II) any State or foreign nation; or (iii) between the District of Columbia and any State, territory, or foreign nation; but (B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45)." *(Source: COPPA).*

Oral Communication

"Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *(Source: ECPA).*

Organized health care arrangement

"(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities: (i) Hold themselves out to the public as participating in a joint arrangement; and (ii) Participate in joint activities that include at least one of the following: (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other

participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. (3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan; (4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or, (5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans." *(Source: HIPAA Regulations)*

Parent

"[A] parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or guardian." *(Source: FERPA Regulations);* "[I]ncludes a legal guardian. *(Source: COPPA).*

Password

"A string of characters used to authenticate an identity or to verify access authorization." *(Source: NIST SP 800-21);* "[C]onfidential authentication information composed of a string of characters." *(Source: HIPAA Regulations)*

Pattern Analysis

"[A] pattern based query that that uses existing intelligence data and detailed models of terrorist activities to search for patterns rather than focusing on uniquely identifiable individuals. *(Source: http://www.heritage.org/Research/HomelandDefense/lm11.cfm).*

Permissioning Systems

"Building privacy rules into databases and search engines through digital rights management and using browsers to enforce privacy principles. These systems show the privacy status of information, highlight compliance requirements for accessing particular data, and support audit functions built into the system." *(Source: http://www.heritage.org/Research/HomelandDefense/lm11.cfm).*

Person

"An individual, organization or entity, but does not include a State or agency thereof." (Source: Drivers Privacy Protection Act); "[A]ny employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." *(Source: ECPA);* "[A]ny individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity." *(Source: FCRA);* "[A]n individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision." *(Source: the Paperwork Reduction Act);* "[A]n individual or a partnership of five or fewer individuals." *(Source: RFPA);* "[A]ny individual, partnership, corporation, trust, estate, cooperative, association, or other entity." *(Source: COPPA).*

Personal Identification Number

"A 4 to 12 character alphanumeric code or password used to authenticate an identity, commonly used in banking applications." *(Source: NIST SP 800-21).*

Personally Identifiable Information (PII)

"[I]ncludes, but is not limited to: (a) The student's name; (b) The name of the student's parent or other family member; (c) The address of the student or student's family; (d) A personal identifier, such as the student's social security number or student number; (e) A list of personal characteristics that would make the student's identity easily traceable or (f) Other information that would make the student's identity easily traceable. *(Source: FERPA Regulations).*

Personal Information

"Information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." *(Source: Drivers Privacy Protection Act);* "[I]ndividually identifiable information about an individual collected online, including— (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph." *(Source: COPPA).*

Physical Safeguards

"Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." *(Source: HIPAA Regulations)*

Plaintext

"Unencrypted (unenciphered) data." *(Source: NIST SP 800-21).*

Privacy Act of 1974

This federal statute controls the collection and dissemination of personal information by the federal government. It guarantees that U.S. citizens and Lawful Permanent Residents have: (1) the right to see records about themselves that are maintained by the federal government (provided that information is not subject to one or more of the Privacy Act's exemptions); (2) the right to amend inaccurate, irrelevant, untimely, or incomplete records; and (3) the right to sue the government for failure to comply with its requirements. It also contains fair information practices that: (1) require that information about a person be collected from that person to the greatest extent practicable; (2) require agencies to ensure that their records are relevant, accurate, timely, and complete; and (3) prohibit agencies from maintaining information describing how an individual exercises his or her First Amendment rights (unless the individual consents to it, it is permitted by statute, or is within the scope of an authorized law enforcement investigation).

Privacy Impact Assessment (PIA)

"An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." *(Source: OMB PIA Guidance).*

Privacy Officer

An official who is responsible for the coordination and implementation of all privacy and confidentiality efforts within a government department or component. This official may be statutorily mandated (e.g., the Department of Homeland Security) or appointed by a Department or component to handle privacy and other related matters.

Privacy Policy In Standardized Machine-Readable Format

"[A] statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser." *(Source: OMB PIA Guidance).*

Private Key

"A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public." *(Source: NIST SP 800-21).*

Profiling

A technique by which information regarding past experiences with a class of persons is used to establish characteristics that are then used to search databases or other records for other persons who closely fit those characteristics.

Protected Computer

Has the meaning set forth in section 1030 of the ECPA. *(Source: ECPA).*

Protected Health Information (PHI)

"Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv)." *(Source: HIPAA Regulations)*

Psychotherapy Notes

"[M]eans notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date." *(Source: HIPAA Regulations)*

Public Health Authority

"An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate." *(Source: HIPAA Regulations)*

Public Key

"A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. [. . .] The public key is used to verify a digital signature. This key is mathematically linked with a corresponding private key." *(Source: NIST SP 800-21).*

Public Information

"Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public." *(Source: Paperwork Reduction Act).*

Public Key Certificate (certificate)

"A set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted third party (certification authority)." *(Source: NIST SP 800-21).*

Public Key Cryptography (reversible)

"Reversible public key cryptography is an asymmetric cryptographic algorithm where data encrypted using the public key can only be decrypted using the private key and conversely, data encrypted using the private key can only be decrypted using the public key." *(Source: NIST SP 800-21).*

Public Key Infrastructure (PKI)

"An architecture which is used to bind public keys to entities, enable other entities to verify public key bindings, revoke such bindings, and provide other services critical to managing public keys." *(Source: NIST SP 800-21).*

Radio Frequency Identification (RFID)

Automated data collection and identification technology that captures data wirelessly and uses radio waves to transmit the signals to a collection device. RFID is similar to bar code technology, but RFID can store more information and has fewer physical limitations than bar code technology.

Readily Accessible to the General Public

"With respect to a radio communication, that such communication is not**:** (A) scrambled or encrypted**;** (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication; (C) carried on a subcarrier or other signal subsidiary to a radio transmission; (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio." *(Source: ECPA).*

Recipient Agency

"Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program." *(Source: Privacy Act)*

Records

"Any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche." (FERPA Regulations); "[A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, /'such as a finger or voice print or a photograph." (Source: Privacy Act and FOIA); "[A]ll books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included." *(Source: OMB A-130 and 44 U.S.C. 3301).*

Recordkeeping Requirement

"[A] requirement imposed by or for an agency on persons to maintain specified records, including a requirement to-- (A) retain such records; (B) notify third parties, the Federal Government, or the public of the existence of such records; (C) disclose such records to third parties, the Federal Government, or the public; or (D) report to third parties, the Federal Government, or the public regarding such records." *(Source: Paperwork Reduction Act).*

Records Disposition

"Any activity with respect to-- (A) disposal of temporary records no longer necessary for the conduct of business by destruction or donation; (B) transfer of records to Federal agency storage facilities or records centers; (C) transfer to the National Archives of the United States of records determined to have sufficient historical or other value to warrant continued preservation; or (D) transfer of records from one Federal agency to any other Federal agency." *(Source: Records Management by the Archivist of the United States)*

Records Maintenance and Use

"Any activity involving-- (A) location of records of a Federal agency; (B) storage, retrieval, and handling of records kept at office file locations by or for a Federal agency; (C) processing of mail by a Federal agency; or (D) selection and utilization of equipment and supplies associated with records and copying." *(Source: Records Management by the Archivist of the United States)*

Records Management

"The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))." *(Source: OMB A-130).*

Records Creation

"The production or reproduction of any record." *(Source: Records Management by the Archivist of the United States).*

Required By Law

"Means a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits." *(Source: HIPAA Regulations)*

Research

"A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." *(Source: HIPAA Regulations)*

Risk

"The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity." *(Source: NIST SP 800-18)*; "The net mission impact considering the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and the resulting impact if this should occur." *(Source: NIST SP 800-47).*

Risk Management

"Is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk." *(Source: NIST SP 800-34).*

Routine Use

"Means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." *(Source: Privacy Act).*

Rules of Behavior

"The rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability." *(Source: NIST SP 800-18).*

Secondary Use

See also: *Mission Creep*

The use of personal information for a purpose different than that for which it was collected.

Secrecy

"Refers to denial of access to information by unauthorized individuals." *(Source: NIST SP 800-21).*

Secret Key

"A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does not imply a classification level, rather the term implies the need to protect the key from disclosure or substitution." *(Source: NIST SP 800-21).*

Security or Security measures

"All of the administrative, physical, and technical safeguards in an information system." *(Source: HIPAA Regulations)*

Security Controls

"Protective measures used to meet the security requirements specified for IT resources." *(Source: NIST SP 800-47).*

Security incident

"The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." *(Source: HIPAA Regulations)*

Sensitive Information

"Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act." *(Source: NIST SP 800-18).*

Sensitivity

"In an information technology environment consists of the system, data, and applications which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components." *(Source: NIST SP 800-18).*

Service Recipient

"An agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor." *(Source: OMB A-130).*

Source Agency

"Any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program." *(Source: Privacy Act).*

State

"Any State, the Commonwealth of Puerto Rico, the District of Columbia, and any territory or possession of the United States." *(Source: FCRA).*

State insurance authority

Means, "in the case of any person engaged in providing insurance, the State insurance authority of the State in which the person is domiciled." *(Source: GLB)*

Statistical Record

"[A] record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of Title 13." *(Source: Privacy Act).*

Student

"Any person with respect to whom an educational agency or institution maintains education records or personally identifiable information, but does not include a person who has not been in attendance at such agency or institution. *(Source: FERPA).*

Supervisory Agency

"With respect to any particular financial institution, holding company, or any subsidiary of a financial institution or holding company, any of the following which has statutory authority to examine the financial condition, business operations, or records or transactions of that institution, holding company, or subsidiary— **(A)** the Federal Deposit Insurance Corporation; **(B)** Director,[1] Office of Thrift Supervision; **(C)** the National Credit Union Administration; **(D)** the Board of Governors of the Federal Reserve System; **(E)** the Comptroller of the Currency; **(F)** the Securities and Exchange Commission; **(G)** the Commodity Futures Trading Commission; **(H)** the Secretary of the Treasury, with respect to the Bank Secrecy Act (Public Law 91–508, title I) [12 U.S.C. 1951 et seq.] and subchapter II of chapter 53 of title 31; or **(I)** any State banking or securities department or agency." *(Source: RFPA).*

System

"[A] generic term used for briefness to mean either a major application or a general support system." *(Source: NIST SP 800-18).*

System Administrator

"A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system administrator would perform systems programmer activities with regard to the operating system and other network control programs." *(Source: NIST SP 800-40).*

System Development Life Cycle

"The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation." *(Source: NIST SP 800-34).*

System Interconnection

"The direct connection of two or more IT systems for the purpose of sharing data and other information resources." *(Source: NIST SP 800-47).*

System of Records

"[A] group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *(Source: Privacy Act).*

Technical Controls

"Hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications." *(Source: NIST SP 800-18).*

Technical Safeguards

"The technology and the policy and procedures for its use that protect electronic protected health information and control access to it." *(Source: HIPAA Regulations)*

Telecommunications

"The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." *(Source: NIST SP 800-59 and 47 USC 5 153).*

Threat

"An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity." *(Source: NIST SP 800-18);* "An entity or event with the potential to harm a system." *(Source: NIST SP 800-21)*; "The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." *(Source: NIST SP 800-47).*

Transaction

"The transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care

claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Other transactions that the Secretary may prescribe by regulation. *(Source: HIPAA Regulations).*

Treatment

"The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another." *(Source: HIPAA Regulations).*

Trojan Horse

"A computer program containing an apparent or actual useful function that also contains additional functions that permit the unauthorized collection, falsification, or destruction of data." *(Source: NIST SP 800-47).*

Use

"With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information." *(Source: HIPAA Regulations)*

User

"Any person or entity who: (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use (Source: ECPA); "[A] person or entity with authorized access." *(Source: HIPAA Regulations).*

Verifiable Parental Consent

"Any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child." *(Source: COPPA).*

Virtual Private Network (VPN)

"A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them." *(Source: NIST SP 800-47).*

Vulnerability

"A flaw or weakness that may allow harm to occur to an automated information system or activity." *(Source: NIST SP 800-18)*; A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. *(Source: NIST SP 800-21)*; A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. *(Source: NIST SP 800-47)*; "A security exposure or mis-configuration in an operating system or other system software or application software component that allows the security policy to be violated. A variety of organizations maintain publicly accessible databases of vulnerabilities based on version number of the software. Much vulnerability can potentially compromise the system or network if successfully exploited." *(Source: NIST SP 800-40).*

Website or Online Service Directed to Children

"(i) "[A] commercial website or online service that is targeted to children; or (ii) that portion of a commercial website or online service that is targeted to children. [. . .] A commercial website or online service, or a portion of a commercial website or online service, shall not be deemed directed to children solely for referring or linking to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link." *(Source: COPPA).*

Wire Communication

"Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." *(Source: ECPA)*

Worm

"A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions." *(Source: NIST SP 800-47)*; "A type of malicious code particular to networked computers. It is a self-replicating program (unlike a virus which needs a host program) which works its way through a computer network exploiting vulnerable hosts, replicating and causing whatever damage it was programmed to do." *(Source: NIST SP 800-40).*

Acknowledgement

The IAPP would like to express its thanks and recognition for the generous contributions of Timothy Skinner and SRA International in compiling this glossary of privacy terminology.

Citations to Sources Referenced Herein:

Federal Statutes

- **Children's Online Privacy Protection Act (COPPA),** 15 U.S.C. Section 6501
- **E-Government Act of 2002,** Public Law 107-347
- **Electronic Communications Privacy Act (ECPA),** 18 U.S.C. Section 2701.
- **Family Educational Right to Privacy Act (FERPA) (aka Buckley Amendment),** 20 U.S.C. Section 1232.
- **Freedom of Information Act (as amended 2002) (FOIA),** 5 U.S.C. Section 552.
- **Gramm-Leach Bliley Act (GLB),** 15 U.S.C. Section 6801.
- **Health Insurance Portability and Accountability Act (HIPAA),** Public Law 105-191.
- **Information Technology Resources Management Act (k/n/a "Clinger-Cohen")**, 40 USC 11101 *et seq.*
- **Paperwork Reduction Act,** 44 U.S.C. Section 3501, Public Law 104-13.

- **Privacy Act of 1974,** 5 U.S.C. § 552A.
- **Records Management by the Archivist of the United States and by the Administrator of General Services**, 44 U.S.C. Section 2901 et seq.
- **Right to Financial Privacy Act (RFPA),** 12 U.S.C. 3401.

OMB Circulars

- **Office of Management and Budget Circular A-130, "Management of Federal Information Resources." (OMB A-130).**

NIST Special Publications

- **NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook (October, 1995).**
- **NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (December, 1998).**
- **NIST Special Publication 800-21 Guideline for Implementing Cryptography in the Federal Government (November, 1999).**
- **NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems (November, 2001).**
- **NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems (June, 2002).**
- **NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, (January, 2002).**
- **NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems (August, 2002).**
- **NIST Special Publication 800-59, Guideline for Identifying an Information System as a National Security System (August, 2003).**