National Institutes of Health

Office of the Senior Official for Privacy

Privacy

Glossary

Table of Contents

Access: Ability to make use of any information system resource. (Defined in NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*)

Access Control: The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). (Defined in FIPS 201-1, *Personal Identity Verification for Federal Employees and Contractors*)

Access Control List (ACL): A register of: (i) users (including groups, machines, and processes) who have been given permission to use a particular system resource; and (ii) the types of access they have been permitted. (Defined in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*)

Accreditation: System security accreditation is the *formal authorization* by the accrediting (management) official for system operation and an *explicit acceptance of risk*. It is usually supported by a review of the system, including its management, operational, and technical controls. This review may include a detailed technical evaluation (such as a Federal Information Processing Standard 102 certification, particularly for complex, critical, or high-risk systems), security evaluation, risk assessment, audit, or other such review. If the life cycle process is being used to manage a project (such as a system upgrade), it is important to recognize that the accreditation is for the entire system, not just for the new addition. (Defined in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook)*

Administrative Controls: Safeguards to ensure proper management and control of information and information systems. These safeguards include policy, the completion of Privacy Impact Assessments (PIAs), certification and accreditation programs, etc. (Defined in NIST SP 800-12, *An Introduction to Computer security: The NIST Handbook*)

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, but does not include: (i) the Government Accountability Office; (ii) the Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. (Defined in 44 U.S.C., Section 3502(1))

Alien: Any person not a citizen or national of the United States. (Defined in 8 U.S.C., Section 1101(a)(3))

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (Defined in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*)

Authorization: The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (Defined in NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems*)

Authorizing Official: A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Authorizing Official Designated Representative: An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Automated Information Security Programs: Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. (Defined in OMB Circular No, A-130, *Management of Federal Information Resources*)

Awareness, Training, and Education: Includes (1) awareness programs that set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) teaching people the skill that shall 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 IT security. (Defined in NIST SP 800-12, Chapter 13, *An Introduction to Computer Security: The NIST Handbook*)

Breach (as it relates to PHI): The unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. (Defined in the *American Recovery and Reinvestment Act of 2009*)

Breach (as it relates to PII): The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. (Defined in OMB Memorandum M-07-16, "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*")

Breach Response Team (BRT): The NIH Breach Response Team engages in risk analysis to determine whether a suspected or confirmed breach of PII poses problems related to identity theft and/or any applicable federal law or policy. If the NIH BRT determines that there has been a breach of PII, the team must assess the risk level associated with the breach, and tailor the agency response accordingly. The NIH BRT coordinates its response with the HHS BRT who may provide further guidance to NIH (e.g., design and execute public outreach efforts) and re-evaluate whether the Department should lead response activities (e.g., those affecting 500 or more individuals). The NIH BRT is comprised of members of the Office of the Director (OD) Office of Management (OM), Office of Management Assessment (OMA/DMS/OSOP), Office of the Chief Information Officer (OD/OCIO/ISAO), Office of Communications and Public Liaison (OCPL) and the Office of General Counsel (OGC). (Defined in NIH Manual Chapter 1745-2, *NIH Incident and Breach Response Policy,* pending release)

Certificates of Confidentiality: The Secretary of HHS may authorize people engaged in biomedical, behavioral, clinical, or other research activities to protect the privacy of research subjects by withholding the names and other identifying characteristics of those subjects from individuals not engaged in the research. Individuals that have such authorization may not be compelled to disclose subjects' names or other identifying characteristics in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding. CoCs may be granted for studies collecting information that, if disclosed, could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. By protecting researchers from being compelled to disclose information that would identify research subjects, CoCs contribute to achieving research objectives and promote participation in studies by helping to ensure confidentiality and privacy to participants. (Defined in Section 301(d) of the *Public Health Service Act*, 42 U.S.C. 241(d))

Certification: A comprehensive assessment of the management, operational and technical security controls in an information system made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operated as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Defined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach)*

Child and Children: An individual under the age of 13. (Defined in *Children's Online Privacy Protection Act (COPPA)* of 1998, Section 1302(1))

Children's Online Privacy Protection Act (COPPA) of 1998: Applies to private sector websites that collect personal information online from children under the age of 13. OMB Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Websites* extended the provisions of *COPPA* to federal websites. COPPA identifies the content that a website operator must include in a privacy policy, outlines when and how to seek verifiable consent from a parent, and specifies the responsibilities an operator has for protecting children's privacy and safety online. (Defined in *Children's Online Privacy Protection Act (COPPA)* of 1998, (15 U.S.C. Section 6501 et seq., 16 CFR, Part 312) (Public Law 105-277) (October 21, 1998)

Clinger-Cohen Act of 1996: Includes both the *Information Technology Management Reform Act* and the *Federal Acquisition Reform Act* and is intended to improve the productivity, efficiency, and effectiveness of federal programs through the improved acquisition, use, and disposal of IT resources. Among other effects, it makes agencies responsible for IT resource acquisition and management, under the guidance of the Chief Information Officer (CIO), and emphasizes that value must be maximized and risk must be minimized in capital planning and budget processes. In effect, the *Clinger-Cohen Act* places the burden of incorporating privacy controls into IT investments at the agency and CIO levels. (Defined in *Clinger-Cohen Act of 1996*, (40 U.S.C. Section 1401) (also known as the *Information Technology Management Reform Act*)

Cloud Deployment Model:

Community Cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Hybrid Cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Public Cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Private Cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. (Defined in NIST SP 800-145, The NIST Definition of Cloud Computing).

Cloud Type:

Broker - An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.

Consumer - A person or organization that maintains a business relationship with, and users services from, cloud providers.

Provider - A person, organization, or entity responsible for making a service available to interested parties. (Defined in NIST SP 500-292, NIST Cloud Computing Security Reference Architecture).

Collaboration: The encouragement of partnerships and cooperation within the federal government, across levels of government and between the government and private institutions to fulfill the agency's core mission activities. (Defined in OMB Memorandum M-10-06, Open Government Directive).

Computer Matching and Privacy Protection Act of 1988: Added several new provisions to the Privacy Act of 1974. "Computer matching" occurs when federal and/or state agencies share information in identifiable form (IIF). Agencies use computer matching to conduct many government functions, including establishing or verifying eligibility for federal benefit programs, or identifying payments/debts owed to government agencies. (Defined in *Computer Matching and Privacy Protection Act of 1988*, (5 U.S.C. 552a(o)). The Act requires agencies engaged in computer matching activities to:

- Provide notice to individuals if their IIF is being computer matched:
- Allow individuals the opportunity to refute adverse information before having a benefit denied or terminated; and
- Establish data integrity boards to oversee computer-matching activities.

Computer Matching Program: 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 computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. (Defined in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations).

Computer Security Act of 1987: Provides a computer standards program within the National Institute of Standards and Technology to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes. (Defined in *Computer Security Act of 1987*, 15 U.S.C. Chapter 7, 40 U.S.C. Section 1441)

Computer Security Incident Response Center (CSIRC): The HHS Computer Security Incident Response Center (CSIRC) is the primary entity in the Department responsible for maintaining Department-wide operational IT security situational awareness and for determining the overall operational IT security risk posture of HHS; a partnership between the HHS CSIRC and Operating Divisions (OPDIVs) for the coordination and execution of incident reporting and response services, and complies with reporting guidelines from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 (as amended), Computer Security Incident Handling Guide and the United States Computer Emergency Readiness Team (US-CERT). (Defined in HHS OCIO, *Policy for Information Technology (IT) Security and Privacy Incident Reporting and Response*)

Computer Security Incident Response Team (CSIRT): The NIH CSIRT identifies, reports, and manages incidents at the NIH level. The CSIRT works with the CISO, SOP and program officials who reported the incident. Additionally, they maintain situational awareness with the HHS PIRT. (Defined in NIH Manual Chapter 1745-2, *NIH Incident and Breach Response Policy*, pending release)

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Defined in NIST SP 800-53, Appendix B, *Recommended Security Controls for Federal Information Systems*)

Contains: To have as contents or constituent parts; to comprise or include. For the purpose of this Guide, the term refers to the collection, use, storage and maintenance of information in IT systems and uses of third-party websites and applications. (Defined in the Webster dictionary).

Contract: A contract is a legal instrument used to reflect a relationship between the Federal Government and the recipient whenever the principle purpose of the transaction is to acquire goods or services for the direct benefit or use of the Government. (Defined in *A Guide to the NIH Acquisition Process 2007*)

Cookie: A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. (Defined in NIST SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*)

a. Authentication Cookie – A cookie that assists the visitor during the login process, by containing the user ID and possibly, password data. A login cookie is typically persistent but may be session-based, and may be linked to other personal information maintained by the Web site. Login cookies tied to a name, account number, or personal e-mail address are considered personally identifiable.

b. Personalization Cookie – A cookie that is used to tailor a Web site based on the past behavior of the visitor. These cookies are not normally tied to a users stated preferences but based on analysis by the Web site on user activity. These cookies are normally persistent.

c. Tracking Cookie – A cookie that is used for aggregate visitor tracking. It is non-personally identifiable and not linked to other logs or information about the visitors that are identifiable. A shopping cart cookie is used to maintain state and associate a visitor with a shopping cart or other transaction thread. These cookies may be linked to PII if the visitor has logged in, is in the checkout process, or is otherwise known. Otherwise, they are often non-personally identifiable.

Data: Programs, files or other information stored in, or processed by, a computer system. (Defined in FIPS PUB 112, *Password Usage*)

Data Asset: 1. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset. 2. An information-based resource. (Defined in Committee on National Security Systems (CNSS) Instruction No. 4009, *National Information Assurance (IA) Glossary*)

Data (Business) Owner: The authority, individual, or organization that has original responsibility for the data by statute, executive order, or directive. (Defined in the *HHS Information Security Program Policy*)

Data Integrity: The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. (Defined in NIST SP 800-27, Appendix A, *Engineering Principles for Information Technology Security, A Baseline for Achieving Security*)

Disclaimer: NIH/IC Web pages containing links to external Web pages not located on NIH servers should include a link to a statement that releases NIH from responsibility for the material included in the external Web pages. It is important to avoid giving a user the impression that NIH is endorsing information, or a commercial product described in an external site. Disclaimers on copyright, endorsement (general and external links), liability, and medical information should be used, as appropriate, for individual IC web sites. In determining appropriate statements, careful consideration should be given to the nature of the specific site and its potential liability. (Defined in NIH OCIO *World Wide Web NIH Guidance*)

Electronic Government Act of 2002: Title II of the E-Government Act of 2002 requires federal agencies to conduct PIAs before developing or procuring IT systems that collect, maintain, or disseminate Information in Identifiable Form (IIF). Once completed, the agency's Chief Information Officer (CIO), or an equivalent official, must review the Privacy Impact Assessments (PIAs). Additional requirements include making PIAs publicly accessible and posting a machine-readable privacy notice on publicly facing websites. (Defined in HHS Cybersecurity Program, *Standard Operating Procedures for Completing a Privacy Impact Assessment* and *E-Government Act of 2002 (E-GOV)* Section 208, (44 U.S.C. Chapter 36)

Electronic Information Collection: Though typically based within a system, an electronic information collection can be an isolated collection of information (such as a survey) set apart from normal system operations. The collection of information must have a PIA performed to determine the risks associated with the collection of the information. (Defined in the HHS-OCIO Policy for Information Systems Security and Privacy).

Encryption: The process of changing plain text into cipher text for the purpose of security or privacy. (Defined in NIST SP 800-57, Part 1, General (Revised) *Recommendation for Key Management)*

Excepted: Records compiled in reasonable anticipation of a civil action or proceeding for which access under the Privacy Act is not granted. (Defined in 5 U.S.C. Section 552a(d)(5) of the *Privacy Act*)

Exempted: Systems of records for which general and specific exemptions can be claimed to prevent release under some requirements of the Privacy Act. (Defined in 5 U.S.C. Section 552a(j)(k) of the *Privacy Act*)

External Links: If an agency posts a link that leads to a third-party Web site or any other location that is not part of an official government domain, the agency should provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a nongovernment Web site that may have different privacy policies from those of the agency's official Web site. (Defined in OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*)

Fair Information Practice Principles (FIPPs): The FIPPs are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies. In a number of organizations, FIPPs serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. In general, privacy controls are implemented within organizations as common controls. (Defined in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations).

Summary of Privacy Control Families:

- Transparency
- Individual Participation and Redress
- Authority and Purpose
- Data Minimization and Retention
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability, Audit, and Risk Management

Federal Acquisition Regulations (FAR): The Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. The Federal Acquisition Regulations System consists of the Federal Acquisition Regulation (FAR), which is the primary document, and agency acquisition regulations that implement or supplement the FAR. (Defined in 48 CFR Federal Acquisition Regulations System, *Federal Acquisition Regulations)*

Federal Information Security Management Act (FISMA) of 2002 (Title III of E-Gov): Provides (1) a comprehensive framework for information security standards and programs and (2) uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. This act defines terms such as information security and information technology and the responsibilities of federal agencies regarding information security. This act also outlines the requirements for annual independent evaluations, which evaluate the effectiveness of an agency's security program and practice. (Defined in HHS-OCIO *Policy for Information Systems Security and Privacy (IS2P)* and *Federal Information Security Management Act (FISMA) of 2002*, (44 U.S.C. Chapter 35)

Federal Record: Includes all 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, decision, procedures, operations or other activities of the Government, or because of the information value of the data in them. (Defined in 44 U.S.C. 3301) (Referenced in HHS policy on Records Management).

Freedom of Information Act (FOIA) of 1966: Requires all agencies of the executive branch to disclose federal agency records or information upon receiving a written request from any individual, except for those records (or portions of them) that are protected from disclosure by certain exemptions and exclusions. FOIA protects the rights of the public to access Government information and makes provisions for individuals to obtain information on the operation of federal agencies. (Defined in *Freedom of Information Act (FOIA) of 1966*, (5 U.S.C 552a, as amended))

General Support System: An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). (Defined in Office of Management and Budget (OMB) Circular A-130, Appendix III (A)(2)(c), *Management of Federal Information Resources*)

Government Furnished Equipment (GFE): Any information processing equipment that is issued by a government agency specifically for government use. This includes, but is not limited to servers, desktops, laptops, Blackberries, personal digital assistants (PDAs), smart phones, and data storage devices. (Defined in CFR 48, Part 45.101, *Federal Acquisition Regulation System*)

Gramm-Leach-Bliley Act of 1999: Includes both a privacy and security component (rule) and applies to persons or organizations (i.e., providers) significantly engaged in financial transactions. (Defined in *Gramm-Leach-Bliley Act of 1999 (GLBA)*, (15 U.S.C. Section 6801-6809))

Health Insurance Portability and Accountability Act (HIPAA) of 1996: Affects the health insurance industry and contains provisions under the heading of "Administrative Simplification" that govern how government and private senior health care institutions handle protected health information (PHI), a subset of "individually identifiable health information." Pursuant with these provisions, regulations published in 2000 established standards for providing notice on how to use and disclose health information collected from users under a covered entity's services. These regulations also grant certain rights to individuals, including the right to see one's health records and to request corrections or other amendments to those records. These regulations apply to both written and oral PHI. (Defined in *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, (42 U.S.C. 1301 et seq.)

Homeland Security Presidential Directive 12 (HSPD-12): Presidential directive requiring the definition of a set of common, acceptable, and achievable standards for Personal Identity Verification (PIV) of Federal employees and contractors. There are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification. (Defined in *Homeland Security Presidential Directive 12, (HSPD-12)* (Aug 27, 2004))

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information that the system possesses, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Defined in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*)

- **Computer Incident** - A violation of imminent threat or violation of computer security policies, acceptable use policies, or standard computer security practices. (Defined in NIST SP 800-61, Appendix D, *Computer Security Incident Handling Guide*)

- **Privacy Incident (formerly referred to as Breach)** - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. (Defined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*)

Incident Response Team (IRT): The NIH Incident Response Team is the frontline information security incident response component of the NIH security program. The IRT provides continuous monitoring and situational awareness reporting to NIH ICs and senior management by promptly and effectively identifying and responding to security incidents, while proactively assuring the security of all NIH systems, data, and biomedical research information through ongoing asset, vulnerability, and configuration scanning. The IRT is comprised of members of the Office of the Chief Information Officer (OD/OCIO/ISAO) and the Center for Information Technology's Division of Network Systems and Telecommunications (CIT/DNST). The Chief Information Security Officer (CISO) participates in or leads incident response processes as a security subject matter expert. The CISO ensures NIH identification, investigative, and incident reporting processes are effective. (Defined in NIH Manual Chapter 1745-2, *NIH Incident and Breach Response Policy*, pending release)

Individual: An individual, for the purposes of the Privacy Act, is an American citizen or an alien lawfully admitted for permanent residence. (Defined in 5 U.S.C. Section 552a(a)(2) of the *Privacy Act*)

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Defined in OMB Circular A-130, 6(j), *Management of Federal Information Resources*)

Information Owner: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. (Defined in NIST SP 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*)

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems (Defined in NIST SP 800-53 Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*).

Information Systems Security Officer (ISSO): An individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Information Technology: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment is considered used by an executive agency if used 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. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (Defined in 40 U.S.C., Section 5002, *Clinger-Cohen Act of 1996*)

Information Technology (IT) System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (Defined in NIST Special Publication 800-53, Revision 3, entitled *Recommended Security Controls for Federal Information Systems and Organizations*). A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected. (Defined in NIST SP 800-16, Appendix C, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*)

Integrity: The degree to which information is timely, accurate, complete, and consistent. Data integrity refers to the quality that is preserved when information and programs are changed only in a specified and authorized manner. System integrity refers to the quality that is demonstrated when a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (Defined in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook)*

Kids' Pages: NIH websites directed to children under the age of 13. "Child" means an individual under the age of 13. (Defined in *Children's Online Privacy Protection Act (COPPA) of 1998*, Section 1302(1))

Machine-Readable Policy: A file that can be read automatically by a web browser or other software agent to enable an end-user to quickly determine a website's privacy practices, and whether that site's privacy practices are in accordance with the end-user's privacy preferences, without the end-user having to read the entire privacy policy. (Defined in the HHS-OCIO Policy for Machine-Readable Privacy Policies).

Maintain: To collect, use or disseminate information. (Defined in 5 U.S.C. Section 552a(a)(3) of the *Privacy Act*)

Major Application: An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, 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 telecommunication components. MAs can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Defined in NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*). All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as a "Major Application." Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d), *Management of Federal Information Resources)*

Major Change: Any change that is made to the system environment or operation of the system. (Defined in OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*). PIAs should be conducted following any major changes, including, but not limited to:

- Conversions: A conversion from paper-based methods to electronic systems;
- Anonymous to Non-Anonymous: When the system's function, as applied to an existing information collection, changes anonymous information into information in identifiable form;
- Significant System Management Changes: In the case that new uses of an existing IT system, including application of new technologies, significantly change the process of managing information in identifiable form in the system;
- Significant Merging: When agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated;
- New Public Access: When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system, which can be accessed by the public;
- Commercial Sources: When information in identifiable form is obtained from commercial or public sources and is systematically integrated into the existing information systems databases;
- New Interagency Uses: When agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form;

- Internal Flow or Collection: When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional information in identifiable form; and
- Alteration in Character of Data: When new information in identifiable form added to a collection raises the risk to personal privacy, such as the addition of health or privacy information.

Make PII Available: Includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. Even individuals who do not have an account with a third-party website or application may make PII available to agencies if certain functions of the website or application are available to individuals without an account. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the Web site or application. "Associate" can include activities commonly referred to as "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions. It is also important to recognize that these activities may make information about a user more widely available than is immediately obvious to the user. For example, a user may post information on one third-party website or application that then may be linked to a different third-party website or application, even without the user's knowledge or consent (Defined in OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*)

Minor Application (child): Minor applications that are considered 'children' are typically included as part of a general support system but require attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (Defined in NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems).

Minor Application (stand-alone): An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (Defined in NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems).

Mobile Devices: Portable cartridge/disk-based removable storage media (e.g., floppy disks, compact disks, USB flash drives, and other flash memory cards/drives that contain non-volatile memory) or portable computing and communication devices with information storage capability (e.g., notebook, laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Need to Know: A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. "Need-to know" and "least privilege" express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (Defined in Committee on National Security Systems (CNSS) Instruction No. 4009, *National Information Assurance (IA) Glossary*)

Non-Exempt System: A Privacy Act system of record for which no exemption is claimed for the system. It typically means the record in the system is releasable to the subject of the file. Naturally, there are some exceptions to the rule. (Defined in 5 U.S.C. Section 552a of the *Privacy Act*)

Nonresident Alien: An individual who is not a citizen or national of the United States and who is in this country on a visa or temporary basis and does not have the right to remain indefinitely. (Defined in 26 U.S.C., Section 7701(b)(1)(B))

Notification: Notification denotes an external communication from any NIH IC, office, or contractor working on behalf of NIH for the purpose of making an affected individual and aware of a breach of their PII. Notification of a breach is also sent, as needed, to entities like healthcare providers, insurers, banks, etc. (Defined in the HHS PII Breach Response Team Standard Operating Procedures).

Paperwork Reduction Act (PRA) of 1995: Focuses on increasing the efficiency of the federal government's information collection practices. The PRA specifies that Chief Information Officers (CIOs) shall improve protection for the privacy and security of information under their agency's control. The PRA also created the Office of Information and Regulatory Affairs (OIRA) within OMB to provide central oversight of information management activities across the federal government. Furthermore, the PRA requires agencies to receive an OMB information collection approval number (also known as an "OMB control number") for an information system, prior to using that system to collect information from any person. (Defined in HHS Cybersecurity Program, *Standard Operating Procedures for Completing a Privacy Impact Assessment (PIA)*) and *Paperwork Reduction Act (PRA) of 1995*, (44 U.S.C. 3501)

Parent: An individual who is the legal guardian of a dependent (i.e., child or young adult). (Defined in *Children's Online Privacy Protection Act (COPPA) of 1998*, (15 U.S.C. Section 6501 et seq., 16 CFR, Part 312)

Participation: The contribution by the public of ideas and expertise so agencies can make policies with the benefit of information that is widely dispersed in society (e.g., links to websites where the public can engage in existing participatory processes, mechanisms, innovative tools and practices that create new and easier methods for public engagement in and feedback on the agency's core mission activities). (Defined in OMB Memorandum M-10-06, Open Government Directive).

Peer-to-peer (P2P): Any software or system allowing individual users of the Internet to connect to each other and trade files. (Defined in OMB M-04-26, *Personal Use Policies and 'File Sharing' Technologies*)

Persistent Cookie: Cookies that collect and maintain information for later use. They can track the activities of users over time and across different websites. These are capable of capturing personal information that can be retrieved by individual identifiers (e.g., name, SSN, etc.) and may therefore be covered by the Privacy Act. (Defined in NIST SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*)

Personal Digital Assistant (PDA) – A handheld computer that serves as a tool for reading and conveying documents, electronic mail, and other electronic media over a communications link, and for organizing personal information, such as a name-and-address database, a to-do list, and an appointment calendar. (Defined in NIST SP 800-124 (Draft), *Guidelines on Cell Phone and PDA Security*)

Personal Identifier: A name, or the identifying number, symbol, or other unique identifier, such as social security number or User ID Number assigned to an individual. (Defined in NIH Manual Chapter 2805, *Web Privacy Policy*)

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, and digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). (Defined in FIPS PUB 201-1, Personal *Identity Verification (PIV) of Federal Employees and Contractors*)

Personally Identifiable Information (PII): Information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. (Defined in OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments)*

Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (Defined in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information)*

Physical Security Controls: Measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data. (Defined in NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*)

Plan of Action and Milestones (POA&M): A tool that identifies tasks that need to be accomplished. POA&MS identify resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (Defined in OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*)

Platform for Privacy Preferences (P3P): A specification created by the World Wide Web Consortium. P3P allows allow users' Web browsers to automatically understand Websites' privacy practices. (Defined in HHS-OCIO, *Policy for Machine-Readable Privacy Policies*)

Privacy: Freedom from unauthorized and unwarranted intrusion. Under the Privacy Act, it is a set of fair information practices to ensure that an individual's personal information is accurate, secure, and current, and that individuals know about the uses of their data. (Defined in 5 U.S.C. Section 552a of the *Privacy Act* and NIST SP 800-32, *Restricting Access to Subscriber or Relying Party Information in Accordance with Federal Law and Agency Policy*)

Privacy Act: Protects the privacy of individuals by establishing "Fair Information Practices" for the collection, maintenance, use, and dissemination of information by federal agencies. The Privacy Act, along with its accompanying case law, is the most significant milestone in the history of the protection of the privacy of personal information held by the federal government. Many subsequent laws, regulations, and guidance build upon the principles first articulated in the Privacy Act. (Defined in HHS OCIO IT 2009-0002.001, *Policy for Privacy Impact Assessment (PIA))*

Privacy Act Record: Any item, collection, or grouping of information about individuals that is maintained by an agency, including, but not limited to, their education, financial transactions, and/or medical, criminal, or employment history and that contains their name; or it contains the identifying number, symbol, or other identifying information assigned to the individual, such as a finger or voice print or a photograph. When the record is under the control of an agency and is contained in an authorized system of records retrieved by personal identifier, it is protected by the provisions of the Privacy Act. **NOTE**: The Privacy Act defines an individual as a U.S. citizen or alien lawfully admitted for permanent residence. Excluded from Privacy Act coverage are the records that Federal agencies maintain on organizations and businesses, including small businesses, even where the company's trade name could be the same as that of the owner. (Defined in 5 U.S.C. Section 552a(a)(4) of the *Privacy Act*)

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. (Defined in OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*)

Privacy Incident Response Team (PIRT): The focal point for privacy incidents, the NIH PIRT identifies incidents, initiates response efforts, and implements corrective actions. The PIRT is comprised of members of the NIH Incident Response Team (IRT), Office of the Chief Information Officer (OD/OCIO/ISAO), and the Office of Management Assessment (OD/OM/OMA/DMS/OSOP). The PIRT Coordinator supports privacy response activities, particularly as they relate to coordinating NIH PIRT interactions. The Senior Official for Privacy (SOP) participates in or leads incident response processes as a privacy subject matter expert. The SOP assists in identifying privacy implications of an incident and provides privacy expertise to response efforts. (Defined in NIH Manual Chapter 1745-2, *NIH Incident and Breach Response Policy*, pending release)

Privacy Notice: A brief description of how the agency's Privacy Policy will apply in a specific situation. Because the Privacy Notice should serve to notify individuals before they engage with an agency, a Privacy Notice should be provided on the specific webpage or application where individuals have the opportunity to make PII available to the agency. (Defined in OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites* and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*)

Privacy Policy: A consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities. Federal agencies must protect an individual's right to privacy when they collect personal information. This is required by the Privacy Act, 5 U.S.C. 552a, and OMB Circular No. A-130, Management of Federal Information Resources. Posting a privacy policy helps ensure that individuals have notice and choice about, and thus confidence in, how their personal information is handled when they use the Internet. Privacy policy in standardized machine-readable format - means a statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a web browser. (Defined in OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites* and OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*)

Privacy Threshold Analysis (PTA): A subset of questions from the PIA form, used to determine whether a complete PIA is required under the E-Government Act. The PIA Summary tab in SPORT serves as the privacy threshold analysis for HHS. (Defined in HHS Cybersecurity Program, *Standard Operating Procedures for Completing a Privacy Impact Assessment)*

Protected Health Information (PHI): "Individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. "Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual;

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The HIPAA Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. (Defined in *Health Insurance Portability and Accountability Act (HIPAA) of 1996*, (42 U.S.C. 1301 et seq.)

Record: Any item, collection, or grouping of information about individuals that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, and/or medical, criminal, or employment history which also contains the their name or an identifying number, symbol, or other identifying information, such as a finger or voice print or a photograph. (Defined in the Privacy Act of 1974, 5 U.S.C., Section 552a(a)(4), as amended).

Registration: Many third-party websites or applications request personally identifiable information (PII) at the time of registration. The process will vary across third-party websites or applications and often users can provide more than is required for registration. For example, users can provide such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown. Agencies should make clear whether they will have access to this information and whether users can take steps to limit agencies' access. (Defined in OMB Memorandum dated December 29, 2011, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications*)

Rehabilitation Act of 1998: Requires agencies to make electronic and IT accessible to people with disabilities, giving employees and members of the public access to information that is comparable to access available to others. (Defined in *Rehabilitation Act of 1998*, Section 508, (29 U.S.C. Section 794d)

Risk: The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. (Defined in NIST SP 800-30, Appendix E, *Risk Management Guide for Information Technology Systems)*

IT-related risks arise from legal liability or mission loss due to:

- Unauthorized (malicious or accidental) disclosure, modification, or destruction of information;
- Unintentional errors and omissions;
- IT disruptions due to natural or man-made disasters;
- Failure to exercise due care and diligence in the implementation and operation of the information system.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. This term is synonymous with risk analysis. (Defined in NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*)

Risk Management: The total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws. (Defined in NIST SP 800-30, Appendix E, *Risk Management Guide for Information Technology Systems)*

Risk Management Framework (RMF): The new six-step process established in NIST SP 800-37 Rev.1, which is the transformation of the previous certification and accreditation (C&A) process. The RMF changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions. (Defined in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*)

Routine Use: Under the Privacy Act, regarding the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected. (Defined in 5 U.S.C. Section 552a(a)(7) of the *Privacy Act*)

Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (Defined in 44 U.S.C., Section 3542, Coordination of Federal Information Policy Subchapter III - Information Security - Definitions).

Security Authorization: See "Authorization." (Defined in NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems*)

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (Defined in NIST SP 800-53; *Recommended Security Controls for Federal Information Systems and Organizations*)

Senior Agency Official for Privacy (SAOP): A title extended by OMB to HHS to effectively meet the reporting requirements outlined in OMB M-06-20, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. (Defined in OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*)

Senior Official for Privacy (SOP): The SOP title was extended by the Department to each OPDIV to effectively meet the reporting requirements outlined in OMB Memorandum M-08-21, FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. (Defined in HHS-OCIO-2010-0006, *Policy for Information Systems Security and Privacy*)

Sensitive Information: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under [the Privacy Act] but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (Defined in *Computer Security Act of 1987*, (15 U.S.C. Chapter 7, 40 U.S.C. Section 1441)

Information is considered sensitive if *the loss of confidentiality, integrity, or availability could be expected to have a* ***serious, severe, or catastrophic*** *adverse effect on organizational operations, organizational assets, or individuals.* Further, the loss of sensitive information confidentiality, integrity, or availability might: (i) cause a significant or severe degradation in mission capability to an extent and duration that the organization is unable to perform its primary functions; (ii) result in significant or major damage to organizational assets; (iii) result in significant or major financial loss; or (iv) result in significant, severe or catastrophic harm to individuals that may involve loss of life or serious life threatening injuries. (Defined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*)

Session Cookie: A small file, stored in temporary memory, containing information about a user that disappears when the user's browser is closed. Unlike a persistent cookie, no file is stored on the user's hard drive. These generally would not save information for later retrieval and would not be covered by the Privacy Act. (Defined in NIST SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*)

Social Media: Includes tools and technologies whose applications are considered new (i.e., recent and emerging) for transferring information and ideas. Though many definitions exist, it is consistently characterized as the collection of web tools that facilitate communication and information sharing. Web-based communities and hosted services include social-networking sites, video and photo sharing sites, wikis, blogs, virtual worlds, and other emerging technologies. (Defined in NIH Manual Chapter 2809, Social and New Media Policy).

Statistical Record: 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. (Defined in 5 U.S.C. Section 552a(a)(6) of the *Privacy Act*)

Submission: An individual can make information available to agencies when he or she provides, submits, communicates, links, posts, or associates PII while using the third-party website or application. This can include such activities as "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions. Individuals who have accounts with third-party websites or applications may transmit PII through the system during the sign-up/log-on transaction or during subsequent interactions. If PII is posted in a public area or sent to the agency in connection with the transaction of public business, it may become a Federal record. (Defined in OMB Memorandum dated December 29, 2011, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications*)

Substance Abuse Records: Records of the identity, diagnosis, prognosis or treatment of any patient maintained in connection with a substance abuse education, treatment, prevention, rehabilitation, training or research program are protected and may only be disclosed under limited circumstances, e.g., to medical personnel with a bona fide need, qualified personnel with a research or management need, or if authorized by a court order upon the showing of substantial risk of death or bodily injury. The statute specifically precludes use of the records to initiate or substantiate a criminal charge or to conduct an investigation. (Defined in *Public Health Service Act*, 42 U.S.C. 290dd-2, Section 543)

System: An organized assembly of IT resources and procedures integrated and regulated by interaction or interdependence to accomplish a set of specified functions. (Defined in HHS Cybersecurity Program, *Standard Operating Procedures for Completing a Privacy Impact Assessment (PIA) Guide*)

System Development Life Cycle (SDLC): A software development process that is used by a systems analyst to develop and maintain an information system. This process includes five system phases: Initiation, acquisition/development, implementation/assessment, operation/maintenance, and disposition. (Defined in NIST SP 800-34, Appendix F, *Contingency Planning Guide for Federal Information Systems*)

System of Records (SOR): A group of any records under the control of any agency where information is retrieved by the name of the individual, by some identifying number or symbol, or other identifiers assigned to the individual. The key to this definition is that the records must be "retrieved by," not "retrievable by" an individual's name and/or personal identifier. **NOTE**: A single document, or group of records that contains publically available information, is not considered a Privacy Act system of records. (Defined in 5 U.S.C. Section 552a(a)(5) of the *Privacy Act*)

System of Records Notice (SORN): All systems with Privacy Act information contained within them are required to publish a "Records Notice" in the Federal Register that informs the public what information is contained in the system, how it is used, how individuals may gain access to information about themselves, and other specific aspects of the system. SORNs can be internal, such as those, which cover NIH records. Central agency SOR notices are those that belong to OPM. Government-wide SOR notices are those that belong to the EEOC, FEMA, GSA, DOL, OGE, etc. and which are referred to as "umbrella" systems of record notices. Before data can be collected, a SORN must be published and maintained in the Federal Register for 40 days. (Defined in *Privacy Act of 1974*, as amended, 5 U.S.C. § 552a(e)(4) and HHS Cybersecurity Program, *Standard Operating Procedures for Completing a Privacy Impact Assessment*)

System Owner/Manager: An agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. The information system owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements. (Defined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*).

Technical Controls: The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. (Defined in NIST SP 800-53, Appendix B, *Recommended Security Controls for Federal Information Systems and Organizations*)

Third-Party Websites and Applications (TPWA): Web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website. (Defined in OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*)

Threat: Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events. (Defined in NIST SP 800-26, Revision A, Appendix A, *Engineering Principles for Information Technology Security* (*A Baseline for Achieving Security*))

Transparency: Providing the public with information about what the agency is doing by making it available online in an open medium or format that can be retrieved, downloaded, indexed, and reached by commonly used web search applications. An open format is one that is platform independent, machine-readable, and made available to the public without restrictions that would impede the re-use of that information (e.g. IC Internet websites, Open Government webpage, Blogs and Social Media websites that request feedback on and assessment of the quality of published information). (Defined in OMB Memorandum M-10-06, Open Government Directive).

Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other IT resource. (Defined in NIST SP 800-61, *Computer Security Incident Handling Guide*)

United States Computer Emergency Response Team (US-CERT): A partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. US-CERT vision is to be a trusted global leader in cybersecurity—collaborative, agile, and responsive in a complex environment. (Defined at http://www.us-cert.gov/)

Usage Tiers: Below are the defined tiers for authorized use of web measurement and customization technologies. (Defined in OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*):

a. Tier 1 – single session**.** This tier encompasses any use of single session web measurement and customization technologies.

b. Tier 2 – multi-session without PII**.** This tier encompasses any use of multi-session web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of such technologies).

c. Tier 3 – multi-session with PII**.** This tier encompasses any use of multi-session web measurement and customization technologies when PII is collected (including when the agency is able to identify an individual as a result of its use of such technologies).

User: Individual, or (system) process acting on behalf of an individual, who is authorized to access an information system. (Defined in Committee on National Security Systems (CNSS) Instruction No. 4009, *National Information Assurance (IA) Glossary*)

Verifiable Parental Consent: Verifiable parental consent means 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. (Defined in *Children's Online Privacy Protection Act* (COPPA) of 1998, (15 U.S.C. Section 6501 et seq., 16 CFR, Part 312)

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Defined in NIST SP 800-53 Rev. 4, *Recommended Security Controls for Federal Information Systems*)

Web Beacon/Bug: A digital object used for web analytics that is placed or embedded in a web page or e-mail to monitor the behavior of the user visiting the website or sending the email. They are used in combination with cookies and are usually transparent graphic images (e.g., invisible to the user). They allow the agency or third party to record simple actions of the user (e.g., track or check that a user has viewed the page or e-mail). When the HTML code for the web beacon/bug points to a site to retrieve the image, at the same time it can pass along information such as the Internet Protocol address of the computer that retrieved the image, the time the web beacon/bug was viewed and for how long, and the type of Internet browser that retrieved the image and previously set the cookie values. Alternative names: Tracking bug, page/pixel tag, clear gif. (Defined in Wikipedia).

Web Measurement and Customization Technologies: These technologies are used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience. (Defined in OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*):

- Single-Session Technologies: These technologies remember a user's online interactions within a single session or visit. Any identifier correlated to a particular user is used only within that session, is not later reused, and is deleted immediately after the session ends.
- Multi-Session Technologies: These technologies remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier for each user, which lasts across multiple sessions or visits.

Website: A collection of interlinked web pages (on either Internet or intranet sites) with a related topic, usually under a single domain name, which includes an intended starting file called a "home page." From the home page, access is gained to all the other pages on the Website. (Defined in HHS Cybersecurity Program, *Standard Operating Procedures for Completing a Privacy Impact Assessment (PIA) Guide*).