Glossary

Overview

If you identify any potential errors in this Glossary or believe we have overlooked a term, please reach out to us at privacy.council@gsa.gov.

General Disclaimer

The definitions of terms provided in this glossary come from official definitions in Federal law, regulation, or Office of Management and Budget policy. The official source of each definition is provided for each term. In many cases, the definitions of terms are specific to a particular law, regulation, or policy and may not apply outside of that context. Agencies shall consult their privacy officials and their counsel when seeking to determine the application or meaning of a term provided in this glossary.

A

Authorization to operate

The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

B

Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).

C

Chief Information Officer

The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Chief Information Officers Council
The Council codified in the E-Government Act of 2002. 44 U.S.C. § 3501 note (Pub. L. 107–347), § 101.

Common Control
A security or privacy control that is inherited by multiple information systems or programs. A control is inherited by an information system when the control is selected for the system but the control is developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Controlled Unclassified Information
Information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Cybersecurity
Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

F

Federal Information
Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Federal Information System
Information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Federal Privacy Council
The Council established by Executive Order 13719. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

H

Health Information
Any information, including genetic 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. 45 C.F.R. § 160.103.

Hybrid Control
A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

I
Incident
An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. 44 U.S.C. § 3552(b)(2).
Individually Identifiable Health Information
Information 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. 45 C.F.R. § 160.103.
Information
Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).
Information in Identifiable Form
Any 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. 44 U.S.C. § 3501 note (Pub. L. 107–347), § 208(d). This includes information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements (i.e., indirect identification). Information 'permitting the physical or online contacting of a specific individual' is the same as 'information in identifiable form.' OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003).
Information Lifecycle
The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).
Information Resources
Information and related resources, such as personnel, equipment, funds, and information technology. 44 U.S.C. § 3502(6).

Information Security
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and c) availability, which means ensuring timely and reliable access to and use of information. 44 U.S.C. § 3552(b)(3).

Information Systems
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 U.S.C. § 3502(8).

Information Technology
Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. The term “information technology” does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. 40 U.S.C. § 11101(6).

O

Open Data
Publicly available data that are made available consistent with relevant privacy, confidentiality, security, and other valid access, use, and dissemination restrictions, and are structured in a way that enables the data to be fully discoverable and usable by end users. Generally, open data are consistent with principles, explained in OMB guidance, of such data being public, accessible, machine-readable, described, reusable, complete, timely, and managed post-release. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

P

Personally Identifiable Information (PII)
Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Continuous Monitoring

'Privacy continuous monitoring' means maintaining ongoing awareness of privacy risks and assessing privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Continuous Monitoring Program

An agency-wide program that implements the agency's privacy continuous monitoring strategy and maintains ongoing awareness of threats and vulnerabilities that may pose privacy risks; monitors changes to information systems and environments of operation that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII; and conducts privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at an agency across the agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Continuous Monitoring Strategy

A formal document that catalogs the available privacy controls implemented at an agency across the agency risk management tiers and ensures that the controls are effectively monitored on an ongoing basis by assigning an agency-defined assessment frequency to each control that is sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Control

The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016)

Privacy Control Assessment

The assessment of privacy controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks. A privacy control assessment is both an assessment and a formal document detailing the process and the outcome of the assessment. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Impact Assessment (PIA)

An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Plan

A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and

describes the methodologies and metrics that will be used to assess the controls. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Privacy Policy

A single, centrally located statement that is accessible from an agency's official homepage. The privacy policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities. OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010).

Privacy Program Plan

A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Program Management Control

'Program management control' means, in the context of information security and privacy, a control that is generally implemented at the agency level, independent of any particular information system, and essential for managing information security or privacy programs. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

Protected Health Information

Individually identifiable health information: (1) except as provided in paragraph (2) of this definition, that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. § 1232g; (ii) in records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years. 45 C.F.R. § 160.103.

Public Information

Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public. 44 U.S.C. § 3502(12).

R

Record

Any 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. 5 U.S.C. § 552a(a)(4).

The term 'records' may also mean all recorded information, regardless of form or characteristics, made or received by a Federal agency 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 United States Government or because of the informational value of data in them. 44 U.S.C. § 3301.

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).

Routine Use

'Routine use' means, with respect to the disclosure of a 'record' (as defined at 5 U.S.C. § 552a(a)(4)), the use of such record for a purpose which is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

S

Senior Agency Official for Privacy

The senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals. OMB M-16-24, Role and Designation of Senior Agency Official for Privacy (September 15, 2016).

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 of the U.S. Code. 5 U.S.C. § 552a(a)(6).

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. 5 U.S.C. § 552a(a)(5).

System-specific Control

A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016).

T

Third-Party Websites or Applications

'Third-party websites or applications' means 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.

OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010).