Elements of a Federal Privacy Program

Overview

Executive Branch agencies are required to have agency-wide privacy programs that, among other things, ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks.

Explore each of **the Elements of a Federal Privacy Program** below to learn more about the various statutory and policy requirements that inform and guide privacy programs.

Please contact privacy.council@gsa.gov with any questions or concerns.

Table of Contents

Breach Response

Overview

It is critically important that Federal agencies remain vigilant and prepare for and understand how to respond to a breach in today's threat landscape. An agency's effective detection and expeditious response to a breach is important to reduce the risk of harm to potentially affected individuals and to keep the public's trust in the ability of the Federal Government to safeguard personally identifiable information (PII).

Related Laws, Policies, and Resources

- Federal Information Security Modernization Act of 2014
  Among other things, the Federal Information Security Modernization Act of 2014 (FISMA) strengthens transparency and accountability, including by making important improvements to the way Federal data breaches are managed and reported to Congress and the public.
- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT

resources, and supporting infrastructure and services. It requires Federal agencies to develop and implement incident management policies and procedures, in accordance with OMB policies and NIST guidelines that address incident detection, response, and recovery.

- OMB's Annual Guidance on Federal Information Security and Privacy Management Requirements
  Among other things, this Memorandum provides agencies with a definition and framework for assessing whether an incident is a major incident for purposes of the Congressional reporting requirements under FISMA. This memorandum also provides specific considerations for determining the circumstances under which a breach constitutes a major incident.
- US-CERT Federal Incident Notification Guidelines (April 1, 2017)
  These guidelines provide guidance to Federal agencies on when to submit incident notifications to the Cybersecurity and Infrastructure Security Agency.
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)
  This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals.

Privacy Impact Assessments

Overview

A privacy impact assessment (or "PIA") is one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and to manage privacy risks. Federal agencies are required to conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle.

Related Laws, Policies, and Resources

- E-Government Act of 2002
  Section 208 of the E-Government Act requires all Federal agencies to conduct a PIA when developing or procuring new information technology involving the collection, maintenance, or dissemination of information in identifiable form or when making substantial changes to existing information technology that manages information in identifiable form.
- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services.
- Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications (December 29, 2011)

This Memorandum includes a model PIA that Federal agencies are required to use when preparing an adapted PIA before engaging the public through third-party websites and applications.

- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010)
  This Memorandum requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public. Among other things, it modifies OMB Memorandum M-03-22 to require an adapted PIA when an agency's use of a third-party website or application makes personally identifiable information available to the agency.
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)
  This Memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002. Among other things, it includes policies and guidelines for when and how to conduct a PIA.

System of Records Notices

Overview

A system of records notice (or "SORN") is published by a Federal agency in the *Federal Register* upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system.

Related Laws, Policies, and Resources

- The Privacy Act of 1974 The Privacy Act of 1974 sets forth a series of requirements governing Federal agency practices with respect to certain information about individuals. Among other things, it requires Federal agencies to publish a SORN in the *Federal Register* that describes the existence and character of a system of records.
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 23, 2016)
  This Circular describes agency responsibilities for implementing the review, reporting, and publication requirements of the Privacy Act of 1974 and related OMB policies. Among other things, it provides guidance to Federal agencies on when to publish a SORN and how to report a system of records to the Office of Management and Budget and to Congress. The Circular requires the use of Office of the Federal Register SORN templates, which are provided in the appendices to the Circular.
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)
  This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of PII. Among other things, it requires Federal agencies to add routine uses

to their system of records notices to cover the disclosure of records when responding to a breach.

- Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975)
  This Circular defines responsibilities for implementing the Privacy Act of 1974 to assure that personal Information about individuals collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon individual privacy. Among other things, it includes guidance on the content of a SORN.

Privacy Workforce

Overview

Agencies' privacy programs play a key role in workforce management activities. The Senior Agency Official for Privacy (SAOP) is required to be involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.

Related Laws, Policies, and Resources

- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Among other things, it requires the SAOP to be involved in assessing and addressing the hiring, training, and professional development needs of the agency with respect to privacy.
- Toolkit for Recruiting, Hiring, and Retaining Privacy Professionals in the Federal Government (January 13, 2017)
  This toolkit is designed to support Federal Government efforts to understand the multidisciplinary nature of the job of a privacy professional and the relevant education, experience, and skills. It is designed to help Federal agency human resource professionals advise organizations in the recruitment and hiring of privacy professionals, and in the career paths available to privacy professionals.

Senior Agency Official for Privacy

Overview

Federal agencies are required to designate a Senior Agency Official for Privacy (SAOP) who has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risks. The SAOP is required to have a central policy-making role and is responsible for ensuring that the agency considers the privacy impact of all agency actions and policies that involve PII. The SAOP is responsible for ensuring that the agency complies with applicable privacy requirements in statute, regulation, and policy.

Related Laws, Policies, and Resources

- Executive Order 13719, Establishment of the Federal Privacy Council (February 9, 2016)
  This Executive Order reinforces the principle that the proper functioning of Government

requires the public's trust, and to maintain that trust the Government must strive to uphold the highest standards for collecting, maintaining, and using personal data. Among other things, it requires the head of each Federal agency to designate a SAOP with the experience and skills necessary to manage an agency-wide privacy program.

- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Among other things, it assigns specific responsibilities to the SAOP associated with the management Federal information resources.
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
  This Memorandum revises policies on the role and designation of the SAOP. Among other things, it establishes requirements governing the designation and responsibilities of the SAOP.

Privacy Risk Management

Overview

Federal agencies' privacy programs have responsibilities under the Risk Management Framework. The Risk Management Framework provides a disciplined and structured process that integrates information security, privacy, and risk management activities into the information system development life cycle.

Related Laws, Policies, and Resources

- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Among other things, it establishes that Federal agencies' privacy programs have responsibilities under the Risk Management Framework.
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control (July 15, 2016)
  This Circular defines management's responsibilities for enterprise risk management (ERM) and internal control. The Circular provides updated implementation guidance to Federal managers to improve accountability and effectiveness of Federal programs and mission-support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. Among other things, it provides considerations for managing privacy risks in Federal programs.
- OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
  This Memorandum revises policies on the role and designation of the SAOP. Among other things, it requires the SAOP to manage privacy risks associated with any agency

activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems.

- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)
  This Memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002. Among other things, it includes policies and guidelines for when and how to conduct a PIA.
  A PIA is 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.
- NIST Special Publication 800-37 (Rev. 2), Risk Management Framework for Information Systems and Organizations (December 20, 2018)
  This Special Publication describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. Among other things, it describes the relationship between information security programs and privacy programs under the RMF.
- NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Information Systems and Organizations (September 23, 2020)
  This Special Publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.
- Collaboration Index for Security and Privacy Controls (XLS) (October 1, 2022)
  This publication serves as a guide to help Federal information security programs and Federal privacy programs understand the level of collaboration that may be appropriate during the implementation step of the National Institute of Standards and Technology (NIST) Risk Management Framework. For each control and control enhancement listed in NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, this publication provides a Collaboration Index value that denotes the level of collaboration that may be appropriate.

Budget and Acquisition

Overview

Federal agencies' privacy programs shall have the resources needed to manage Federal information resources that involve personally identifiable information (PII). This will require privacy programs to play a key role in the development of the agencies' budget requests, as well as any decisions to acquire or develop information system technologies and services.

Related Laws, Policies, and Resources

- E-Government Act of 2002
  Section 208 of the E-Government Act requires all Federal agencies to conduct a privacy impact assessment (PIA) when developing or procuring new information technology involving the collection, maintenance, or dissemination of information in identifiable form or when making substantial changes to existing information technology that manages information in identifiable form. Among other things, it requires Federal agencies to provide the Director of the Office of Management and Budget with a copy of the PIA for each system for which funding is requested.
- OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget
  This Circular provides guidance on preparing, submitting, and executing the President's Budget. Among other things it requires Federal agencies' Chief Information Officers to collaborate with Senior Agency Officials for Privacy (SAOP) on their IT Budget submissions. It requires Federal agencies to include in their IT Resource Statements a statement that the SAOP has reviewed the IT Budget submission and that privacy requirements, as well as any associated costs, are explicitly identified and included with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.
- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Among other things, it requires privacy programs to play a key role in the development of the agencies' budget requests, as well as any decisions to acquire or develop information system technologies and services.

Websites and Digital Services

Overview

Federal agency public websites and digital services are the primary means by which the public receives information from and interacts with the Federal Government. These websites and services help the public apply for benefits, search for jobs, comply with Federal rules, obtain authoritative information, and much more. Federal websites and digital services should always meet and maintain high standards of effectiveness and usability and provide quality information that is readily accessible to all.

Related Laws, Policies, and Resources

- E-Government Act of 2002
  Section 208 of the E-Government Act requires the Director of the Office of Management and Budget to develop guidance on notices for Federal agency websites used by the public.
- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT

resources, and supporting infrastructure and services. Among other things, it requires Federal agencies to maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy.

- OMB Memorandum M-23-22, Delivering a Digital-First Public Experience (September 22, 2023)
  This Memorandum provides guidance to agencies on how to design and deliver websites and digital services to the public and to assist agencies as they continue to implement the 21st Century Integrated Digital Experience Act. Among other things, it requires Federal agencies to maintain a central resource page dedicated to its privacy program on the agency's principal website.
- OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010)
  This Memorandum requires Federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public. It also applies when a Federal agency relies on a contractor (or other non-Federal entity) to operate a third-party website or application to engage with the public on the agency's behalf.
- OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010)
  This Memorandum provides updated guidance and requirements for agency use of web measurement and customization technologies. Web measurement and customization technologies are technologies that are used to remember a user's online interactions with a website or online application in order to measure and analyze usage or to customize the user's experience.
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)
  This Memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002. Among other things, it includes guidance for privacy policies on Federal agencies' websites used by the public.
- OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999)
  This Memorandum requires Federal agencies to post privacy policies on agency websites. Among other things, it includes guidance and model language for Federal website privacy policies.

Training and Accountability

Overview

Federal agencies are required to establish rules of behavior for employees and contractors with access to personally identifiable information (PII) and hold agency personnel accountable for complying with applicable privacy requirements and managing privacy risks. This necessarily requires developing, maintaining, and providing agency-wide privacy awareness and training programs for all employees and contractors.

Related Laws, Policies, and Resources

- Executive Order 13719, Establishment of the Federal Privacy Council (February 9, 2016)
  This Executive Order establishes the Federal Privacy Council as the principal interagency forum to improve the privacy practices of Federal agencies and entities acting on their behalf. Among other things, it requires the Federal Privacy Council to assess and recommend how best to address the hiring, training, and professional development needs of the Federal Government with respect to privacy matters.
- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
  This Circular establishes general policy for the planning, budgeting, governance, acquisition, and management of Federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Among other things, it requires Federal agencies to develop, maintain, and provide agency-wide privacy awareness and training programs for all employees and contractors.
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)
  This Memorandum sets forth the policy for Federal agencies to prepare for and respond to a breach of PII. Among other things, it requires Federal agencies to establish rules of behavior, including consequences for violating such rules, for employees, contractors, and others who have access to Federal information or information systems.
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)
  This Memorandum provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002. Among other things, it requires Federal agencies to inform and educate employees and contractors of their responsibility for protecting PII.