Congressional Research Service
Informing the legislative debate since 1914

Access to Agency Data and Information Technology: Frequently Asked Questions

February 12, 2025

Congressional Research Service
https://crsreports.congress.gov
R48423

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Access to Agency Information Technology: Frequently Asked Questions

Congressional interest in the information technology (IT) that generates, stores, manipulates, transmits, and disposes of data used by federal agencies has increased since the beginning of the 119th Congress. This CRS Frequently Asked Questions report provides background information to congressional staff related to access to federal information and the security IT systems.

This report covers information on federal IT management, the cybersecurity of federal IT systems and data, the privacy of federal information, federal data integration, and the management of federal records.

SUMMARY

R48423

February 12, 2025

Chris Jaikaran, Coordinator
Specialist in Cybersecurity Policy

Dominick A. Fiorentino
Analyst in Government Organization and Management

Natalie R. Ortiz
Analyst in Government Organization and Management

Meghan M. Stuessy
Analyst in Government Organization and Management

Contents

Appendixes

Contacts

Introduction

Congressional interest in the information technology (IT) that generates, stores, manipulates, transmits, and disposes of data used by federal agencies has increased since the beginning of the 119th Congress. This CRS Frequently Asked Questions report provides background information to congressional staff related to access to federal information and the security IT systems.

This report covers information on federal IT management, the cybersecurity of federal IT systems and data, the privacy of federal information, federal data integration, and the management of federal records.

Information Technology Management

Information Technology is defined by Title 40, Subtitle III, of the *U.S. Code* as:

> any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.[1]

IT systems serve as a means by which federal agencies interact with citizens, other federal agencies, state and local governments, and the private sector (such as contractors providing goods and services to the federal government), and play an important role in government operations, including:

- providing services directly to the public;
- running the back-office operations of agencies;
- maintaining records of government activities; and
- providing information to Congress and the public about the activities of agencies and the President.

What laws govern IT management and budgeting?

Several key pieces of legislation have shaped the agency IT management and budgeting. Practitioners often refer to these statutes by their original short titles, even though many of the statutory provisions are now located in different parts of the *U.S. Code*.

Clinger-Cohen Act of 1996

The Clinger-Cohen Act of 1996 (P.L. 104-106, Divs. D and E) emerged from growing concern about the federal government's ability to develop and maintain IT infrastructure and personnel.[2] In 1994, a subcommittee of the Senate Committee on Governmental Affairs detailed what it described as systemic problems in federal IT procurement and ineffective oversight of IT programs.[3] Clinger-Cohen extensively modified federal IT acquisition policy and procurement

[1] 40 U.S.C. §11101.

[2] The law, as subsequently retitled by P.L. 104-208 (110 Stat. 3009-393), comprised Divisions D (110 Stat. 642) and E (110 Stat. 679) of P.L. 104-106 (110 Stat. 186), at https://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf.

[3] As the ranking minority member of the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Sen. William Cohen directed a staff study of major government IT integration and (continued...)

management. In doing so, it assigned certain IT management roles and responsibilities to agency Chief Information Officers (CIOs), including development and maintenance of IT systems and evaluation, assessment, and reporting on IT improvements.[4] Additionally, Clinger-Cohen established a new federal IT capital planning and investment control process, with prominent roles for OMB and agencies.[5]

E-Government Act of 2002

Building on the provisions enacted under the Clinger-Cohen Act, the E-Government Act of 2002 (P.L. 107-347) sought to improve federal IT investment and management.[6] The E-Government Act enacted into law several provisions related to IT management including:

- delegating IT procurement responsibilities to agencies, and establishing a new federal IT capital planning and investment control process, with prominent roles for OMB and agencies;
- redesignating agency "senior officials" responsible for the coordination of federal information policy as Chief Information Officers, and making agency CIOs responsible for developing and maintaining IT systems as well as evaluating, assessing, and reporting on IT improvements;[7] and
- establishing the Office of Electronic Government within OMB.[8]

In practice, OMB refers to this organization as the Office of the Federal Chief Information Officer (OFCIO).[9] OFCIO is responsible for providing overall leadership for the executive branch on electronic government as well as setting IT standards and guidelines for executive branch agencies.[10] To implement these statutory requirements, OFCIO helps develop OMB memoranda, circulars, and strategy documents to guide executive branch agencies on developing and implementing IT standards, IT workforce plans, and IT capital plans, among other policies.

modernization efforts in progress. See U.S. Sen. William S. Cohen, *Computer Chaos: Billions Wasted Buying Federal Computer Systems, Investigative Report*, report from minority staff of the Senate Subcommittee on Oversight of Government Management (Washington: October 12, 1994).

[4] See CRS Report RL30661, *Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act)*, by Jeffrey W. Seifert (out of print; available to congressional clients upon request).

[5] Ibid.

[6] See "E-Government Act of 2002," by Harold C. Relyea and Jeffrey W. Seifert, in CRS Report RL30795, *General Management Laws: A Compendium*, by Clinton T. Brass et al. (out of print; available to congressional clients upon request).

[7] P.L. 104-106, §5125, 110 Stat. 684. The Paperwork Reduction Act of 1980 (P.L. 96-511, 94 Stat. 2819) required each agency head to designate a "senior official" to report directly to the agency head and carry out responsibilities related to the coordination of federal information policy.

[8] P.L. 107-347, December 17, 2002; 116 Stat. 2899, at 2902. Relevant provisions are codified at Title 44, Section 3602, of the *U.S. Code* at https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.

[9] OMB, "Office of the Federal Chief Information Officer," https://bidenwhitehouse.archives.gov/omb/management/ofcio/.

[10] 44 U.S.C. §3602.

Federal Information Technology Acquisition Reform Act (2014)

In 2014, the Federal Information Technology Acquisition Reform Act (FITARA, P.L. 113-291, Title VIII, Subtitle D) built upon the Clinger-Cohen Act to establish a framework for tracking, assessing, and managing federal IT investments.[11] Provisions related to IT budgeting include:

- increasing transparency of IT investments;[12]
- establishing requirements for categorizing IT investments according to risk;[13] and
- establishing requirements for an agency IT portfolio review process, where individual investments are viewed in the context of the agency's broader set of projects.[14]

How can I track agency IT investments?

OMB created its IT Dashboard website in 2009 to increase transparency of agency IT investments.[15] In 2014, FITARA made aspects of this administrative practice a statutory requirement.[16] The resulting publicly-accessible website displays data from 26 agencies on the cost, schedule, and performance of IT investments. In 2022, management of the IT Dashboard was transferred from OMB to the General Services Administration (GSA).[17] In addition to agency-wide data, the dashboard now includes individual IT investment spending and detailed performance metrics. Investment details include schedule status, schedule variances, spending totals, personnel full-time equivalents, cost variances, CIO risk ratings, investment goals, and contracts associated with the investment.[18]

Cybersecurity

Cybersecurity is a risk management process rather than an end-state. It involves continuous work to identify and protect against potential cybersecurity incidents; and to detect, respond to, and recover from actual cybersecurity incidents. Agencies may choose to evaluate their IT risks by understanding the threats they are susceptible to, the vulnerabilities they have, and the potential consequences a successful attack might have for their mission and their customers.

What laws govern the cybersecurity of federal IT systems?

The Computer Security Act of 1987 (P.L. 100-235) directed the Secretary of Commerce to work with the National Security Agency (NSA) to create standards and guidance for the protection of

[11] P.L. 113-291, Title VIII, Subtitle D, of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015; 128 Stat. 3438.

[12] 40 U.S.C. §11302(c)(3)(A).

[13] 40 U.S.C. §11302(c)(3)(C).

[14] 40 U.S.C. §11319.

[15] The IT Dashboard website is located at https://itdashboard.gov/.

[16] 40 U.S.C. §11302(c)(3)(A).

[17] General Services Administration (GSA), "GSA Launches Modernized Federal IT Dashboard to Enhance Transparency and Accountability in Federal IT Modernization," March 21, 2022, https://www.gsa.gov/about-us/newsroom/news-releases/gsa-launches-modernized-federal-it-dashboard-to-enhance-transparency-and-accountability-in-federal-it-modernization-03212022.

[18] GSA, IT Dashboard, "IT Portfolio Dashboard," https://www.itdashboard.gov/itportfoliodashboard.

federal computer systems.[19] The Information Technology Management Reform Act of 1996 (P.L. 104-106, Title LI) required the National Institute of Standards and Technology (NIST) to promulgate compulsory standards to improve the security and privacy of federal computer systems.[20]

The Federal Information Security Modernization Act of 2014 (FISMA, P.L. 113-283) establishes roles and responsibilities for federal agency IT security.[21] This act functionally updates the original Federal Information Security Management Act of 2002 (Title III of the E-Government Act of 2002, P.L. 107-347). FISMA states that while agency heads are ultimately responsible for the security of their agency's IT, they may delegate these responsibilities to a senior agency official. In implementing their IT security programs, agencies must follow guidance issued by the Office of Management and Budget (OMB) and standards promulgated by NIST. Each agency's inspector general (IG) must produce an annual evaluation of the agency's cybersecurity. The 2014 version of FISMA added a role for Department of Homeland Security (DHS): authorizing it to assist agencies in their IT security programs. DHS executes this role through one of the department's components: the Cybersecurity and Infrastructure Security Agency (CISA).

Are there penalties for violating FISMA?

FISMA was designed to provide clarity for IT security responsibilities. FISMA is silent on penalties and is not self-enforcing. Agencies determine appropriate access and use of their technology. If a system owner determines that an authorized user has misused a federal system, then the agency could take action. Potential remediations include additional training for employees, revocation of access, reprimands of federal employees, or removal of contractors (based on the parameters of the contract).

Who is responsible for determining appropriate access to a system?

Agency officials with jurisdiction over an IT system may determine which individuals can have access to that system. These officials may include (but are not limited to) agency leaders (e.g., secretaries, assistant secretaries, and administrators), the authorizing official for that system, the system owner, or the system's program manager.

What other documents govern agency cybersecurity programs?

Agencies use several different standards and guidance documents to inform their IT security programs. These documents are generally required of agencies. In certain cases, agencies may request waivers to avoid or delay compliance. Some of the main documents are listed below.

- OMB Circular A-130 on *Management of Federal Information Resources.*
- OMB Memoranda on implementing FISMA, such as M-25-04 on *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements.*
- The Chief Information Officers Council Handbook and the Chief Information Security Officer Handbook.

[19] The Computer Security Act of 1987 were updated in 2003 with the passage of the Federal Information Security Management Act (P.L. 107-347) and the Federal Information Security Modernization Act of 2014 (P.L. 113-283). Both acts are referred to as FISMA and can be found in 44 U.S.C. Chapter 34, Subchapter II.

[20] 40 U.S.C. §11331.

[21] 44 U.S.C. §§3551-3559.

- Federal Information Processing Standards (FIPS), such as FIPS-199 on *Standards for Security Categorization of Federal Information and Information Systems* and FIPS-200 *Minimum Security Requirements for Federal Information and Information Systems.*
- NIST Special Publications (SPs), such as SP 800-53r5 on *Security and Privacy Controls for Information Systems and Organizations* and SP 800-171r3 on *Protecting Controlled Unclassified Information on Nonfederal Systems and Organizations.*
- DHS Binding Operational Directives (BODs), such as BOD 18-02 on *Security High Value Assets.*

Agencies also have agency-specific documents—such as information system security authorization guidance—that they must follow.

Are there types of federal government data that carry additional access controls?

Yes, certain data carry further restrictions around its access and use. Those restrictions are established in the authorizing statute for the data itself. Some examples of this type of data include social security and tax information. Other information is further protected by agency policy. The National Archives and Records Administration (NARA) maintains a list of controlled unclassified information.[22] National security information (i.e., classified information) carry additional protections from unauthorized disclosure in statute and policy.[23]

Privacy

By law, government agencies are required to follow certain privacy processes with respect to agency records containing individually identifying information, such as how these records are to be stored, who may access information in the records, when the government may use or disclose that information, and how risk to records systems is assessed and documented. Information concerning individuals (such as name, social security number, biometric records) is sometimes referred to as *personally identifiable information*, or PII.[24] These laws include the E-Government Act of 2002 (P.L. 107-347) and the Privacy Act of 1974 (Privacy Act, P.L. 93-579).[25] Neither the E-Government Act of 2002 nor the Privacy Act uses the phrase PII; instead, the E-Government Act discusses *identifiable form*, and the Privacy Act pertains to individually identifying information.[26]

[22] National Archives, "CUI Categories," January 31, 2024, https://www.archives.gov/cui/registry/category-list.

[23] For more information on classified information, see CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*, by Jennifer K. Elsea.

[24] OMB, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," M-07-16, May 22, 2007, p. 1, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2007/m07-16.pdf. On June 15, 2007, OMB incorporated this definition of *personally identifiable information* in its guidance on implementation of Title V of the E-Government Act of 2002 and the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA); see 72 *Federal Register* 33362-33377. S. 116, introduced in 2005 during the 109th Cong., appears to be the first legislative instance of the term *personally identifiable information*. However, the bill was not enacted. In the years since CIPSEA's implementation, Congress may consider whether OMB's response is still sufficient.

[25] 5 U.S.C. §552a.

[26] For more information, see "Identifying Particulars and Personally Identifiable Information (PII)" in CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy.

With respect to privacy, the E-Government Act requires federal agencies to conduct privacy impact assessments (PIAs) when developing or procuring IT systems that collect, maintain, or disseminate information in a potentially identifiable form.[27] The Privacy Act generally restricts the disclosure of information concerning individuals without the individual's prior written consent and requires agencies to describe elements of their systems containing PII in publicly available systems of records notices (SORNs). The Privacy Act also contains criminal penalties for violating the act. Additional provisions of the Privacy Act, known as the Computer Matching and Privacy Protection Act (CMPPA; P.L. 100-503), use and build upon the definitions of the Privacy Act for the purposes of conducting *matching programs*.

What is a Privacy Impact Assessment (PIA)?

A PIA documents the information a system will collect, use, store and share, as assessed by an agency. Section 208 of the E-Government Act of 2002 requires federal agencies to conduct PIAs to ensure sufficient privacy protections of personal information when the information is in an identifiable form.[28] Per statute, PIAs are to be reviewed by the agency CIO or equivalent official (as determined by the head of the agency.)[29] By statute, elements required to be addressed in a PIA include:

- what information is to be collected;
- why the information is being collected;
- the information's intended agency use;
- with whom the information will be shared;
- what notice or opportunities for consent would be provided to individuals regarding information collection and sharing;
- how the information will be secured; and
- whether a system of records is being created.[30]

Further, the act defines *identifiable form* as "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."[31] OMB Memorandum M-03-22, which provides guidance to agencies implementing the E-Government Act of 2002, explains that a PIA is required to be performed and "updated as necessary" when a system change creates new privacy risks, including, for example, (1) when agencies convert paper-based records to electronic systems, (2) when functions applied to an existing information collection change anonymous information into information in

[27] 44 U.S.C. §3501 note.

[28] P.L. 107-347; 116 Stat. 2899. Section 208 of the E-Government Act of 2002 is located in chapter 35 of Title 44, Section 3501 note, of the *U.S. Code*. Chapter 35 of Title 44 focuses on OMB coordination of federal information policy, as opposed to the broader administrative procedure statutes of Title 5 of the *U.S. Code*, where provisions associated with FOIA and the Privacy Act are located. The act's Title 44 location underscores the role of OMB to guide information policy as informed by the Privacy Act.

[29] 44 U.S.C. §3501 note; P.L. 107-347, 116 Stat. 2922.

[30] 44 U.S.C. §3501 note. Example PIA templates may be viewed at Consumer Financial Protection Bureau, "Privacy Impact Assessment Template," https://files.consumerfinance.gov/f/documents/cfpb_pia-template.pdf, and U.S. Department of Commerce, *Privacy Impact Assessment Template*, https://www.osec.doc.gov/opog/privacy/PIA_Template.pdf.

[31] 44 U.S.C. §3501 note; P.L. 107-347, 116 Stat. 2923.

identifiable form, or (3) when agencies adopt or alter business processes to allow for the merging, centralization, or matching of information with other databases.[32]

In 2010, OMB provided additional guidance on PIAs for agency use of third-party websites and applications.[33] Congress might evaluate whether the current statute and guidance are sufficient given the evolution in information management since the law's passage in 2002. Additionally, Congress may inquire whether agency staff has been given sufficient training or guidance from OMB to understand when new collections, format changes, or modifications to information could create privacy risks that would necessitate an updated PIA.

What is the Privacy Act of 1974?

In brief, the Privacy Act of 1974 governs federal agencies' access, use, and disclosure of information concerning individuals. With 12 exceptions, information on individuals may not be disclosed without the prior written consent of the individual. The statute also provides 10 exemptions for categories of records about individuals that are outside the scope of the Privacy Act's protections.

Specifically, the act concerns *agency* uses of an *individual's records* that are maintained and retrieved within a *system of records*. Descriptions of these key terms, from both statute and DOJ guidance, are provided below.

- **Agency.** The Privacy Act uses the Freedom of Information Act's (FOIA) definition of *agency*.[34] This definition covers executive branch agencies, their components, and government-controlled entities but excludes Congress, the legislative branch, the White House, federal courts, and state and local governments.[35]
- **Individual.** An *individual* is defined in the act as "a citizen of the United States or an alien lawfully admitted for permanent residence."[36] This definition excludes deceased persons, corporations, or organizations. In certain instances, parents or legal guardians may act on behalf of individuals.[37]
- **Record.** Statute defines *record* as "any item, collection, or grouping of information about an individual that is maintained by an agency" that contains

[32] OMB, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," M-03-22, September 26, 2003, p. 4, https://www.bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf.

[33] Kevin Neyland, *Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications*, OMB, December 29, 2011, https://www.bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf.

[34] 5 U.S.C. §552a(a)(1); 5 U.S.C. §552(f)(1).

[35] The definitions of the Privacy Act have been discussed and interpreted in various court cases. DOJ summarizes relevant caselaw in its *Overview of the Privacy Act*. For a discussion of the definition of *agency*, see DOJ, *Overview of the Privacy Act of 1974*, pp. 15-17, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition. Please note that determining when information becomes an *agency* record may have implications regarding the government's use and purchase of information created by contractors or collected by third parties, such as data brokers. For more information on the federal procurement process and contracting, see CRS Report RS22536, *Overview of the Federal Procurement Process and Resources*, by Dominick A. Fiorentino. For more information on how consumer data may be collected by data brokers, see CRS Report R47298, *Online Consumer Data Collection and Data Privacy*, by Clare Y. Cho and Ling Zhu.

[36] 5 U.S.C. §552a(a)(2).

[37] DOJ, *Overview of the Privacy Act of 1974*, 2020, pp. 23-26, https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition.

the individual's name, identifying number, or other identifying particular assigned to the individual.[38] Courts have variously interpreted how closely associated the information needs to be with an individual to count as a record for purposes of the Privacy Act.[39] Like FOIA, the Privacy Act pertains only to federal information, and most courts have held that it does not require agencies to create records.[40]

- **System of Records.** A *system of records* is a "group of any records under the control of any agency" from which the information is retrieved by the name of the individual or other identifying particular.[41]

When can information be shared without an individual's written consent?

The Privacy Act generally prohibits disclosure of individually identifiable information to third parties without written consent. Specifically, an agency may not disclose a record to a third party without the individual's prior written consent unless such a disclosure falls under one of 12 exceptions in Title 5, Section 552a(b), of the *U.S. Code*.[42]

Three of the exceptions may be of particular interest as they pertain to access to agency IT systems and data.[43] First, the Privacy Act permits an agency to disclose covered information with other employees of the same agency who have a *need to know* the information in the performance of their duties. Second, an agency can disclose information to the public if FOIA requires its disclosure. Third, an agency may disclose information if the purpose of the disclosure is a *routine use* of the information. A routine use, under the Privacy Act, is "use of such record for a purpose which is compatible with the purpose for which it was collected" and may include the sharing of information across agencies.[44] Routine uses are documented in the *Federal Register* in an agency's system of records notice.

What is a System of Records Notice?

For purposes of the Privacy Act, an agency may control a group of records where information is retrievable by an individual's name or other unique identifiers. This group of records is referred to as a *system of records*.[45] When an agency seeks to establish a new system of records or make significant changes to an existing system of records, the act requires the agency to submit a

[38] 5 U.S.C. §552a(a)(4).

[39] DOJ, *Overview of the Privacy Act of 1974*, pp. 28-36.

[40] DOJ, *Overview of the Privacy Act of 1974*, p. 37.

[41] 5 U.S.C. §552a(a)(5) and DOJ, *Overview of the Privacy Act of 1974*, p. 37. According to DOJ, in exploring the idea of retrieval, "The statutory definition of a 'system of records' requires that: (1) 'there is an indexing or retrieval capability using identifying particulars built into the system'; and (2) the agency 'does, in fact, retrieve records about individuals by reference to some personal identifier.'" See also OMB, "Privacy Act Implementation: Guidelines and Responsibilities," 40 *Federal Register* 28948 and 28952, July 9, 1975.

[42] 5 U.S.C. §552a(b). For discussion of these exceptions, see DOJ, *Overview of the Privacy Act: 2020 Edition*, "Conditions of Disclosure to Third Parties," https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/disclosures-third-parties. A full list of these exceptions is located in the Appendix of CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy.

[43] For more discussion of these exceptions, see "12 Exceptions to Written Consent" in CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy.

[44] 5 U.S.C. §552a(a)(7).

[45] 5 U.S.C. §552a(a)(5).

proposal to OMB and Congress.[46] OMB explains that a "significant change" that would require submission of a revised SORN could include:

- a substantial increase in the number, type, or category of individuals about whom the records are maintained in the system, or a change that expands the types or categories of records in the system;
- a change that modifies the scope of the system or the purpose for which the information is maintained; and
- a new routine use or significant change to an existing routine use of that system.[47]

After review by and potential comments from OMB, the agency publishes a SORN in the *Federal Register* and provides 30 days for the public to submit written views on the proposed use of the system.[48] A typical SORN must include information such as:

- the name and location of the system;
- the categories of records and individuals on whom records are maintained;
- each routine use of the records contained in the system, including the categories of users and the purpose of such use; and
- the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.[49]

Certain systems of records may be exempted from selected Privacy Act requirements by an agency head based on the system's contents, subject to notice of the proposed exemption in the *Federal Register*.[50]

Are there penalties for violating the Privacy Act?

The Privacy Act provides for certain civil remedies and criminal penalties in the event the act is violated.[51] The Department of Justice describes the civil remedies as comprising two categories:

[46] 5 U.S.C. §552a(r). The proposal is to enable "an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals." See also OMB, "Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act," December 23, 2016, p. 14, https://www.bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf.

[47] OMB developed a list of examples of significant changes requiring a revised SORN at OMB, "Circular No. A-108," pp. 5-6.

[48] 5 U.S.C. §552a(e)(11). OMB guidance indicates that a SORN is considered in effect upon publication in the *Federal Register* with the exception of "any new or significantly modified routine uses." OMB further explains, "Agencies shall publish notice of any new or significantly modified routine use sufficiently in advance of the proposed effective date of the routine use to permit time for the public to comment and for the agency to review those comments. In no circumstance may an agency use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following *Federal Register* publication." OMB, "Circular No. A-108," p. 7. For a brief description of the OMB director's government-wide roles under the Privacy Act, see OMB, "Circular No. A-108," p. 31.

[49] 5 U.S.C. §552a(e)(4). See also OMB, "Circular No. A-108," p. 16. OMB provides SORN templates in Appendices II, III, and IV of Circular No. A-108.

[50] 5 U.S.C. §§552a(j) and 552a(k). For discussion of statutory provisions that explicitly exempt or allow agencies to exempt certain categories of records (or information within records) from certain Privacy Act provisions, see DOJ, *Overview of the Privacy Act of 1974*, pp. 338-372, and OMB, "Circular No. A-108," p. 25.

[51] 5 U.S.C. §§552a(g) and 552a(i).

causes of action that provide for injunctive relief, and causes of action that provide for compensatory relief in the form of monetary damages.[52]

Certain criminal penalties may be levied against officers or employees of an agency, while another may be levied against persons. Per statute:

> (1) Criminal Penalties.-Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
>
> (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.
>
> (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.[53]

Federal Data Integration

Computers and information technologies have increased the amount of data that can be collected, stored, and processed. Computers make it easier to exchange, share, and match data on individuals across programmatic and agency boundaries, enabling the use of that data for various executive branch operations. Congress has deliberated and legislated the use of data integration for more than 50 years, aiming to promote the efficient administration of government programs while protecting individual privacy and maintaining the country's trust in how the federal government uses information on individuals.

The Computer Matching and Privacy Protection Act (CMPPA; P.L. 100-503) is a significant part of the statutory and policy landscape and shapes how agencies can share and combine data sources that concern individuals. The CMPPA emerged from congressional concerns that the oversight of agency data matching was inadequate. In particular, the extent of data matching in the executive branch was unknown, and the due process rights of individuals were not adequately protected from adverse actions by an agency using inaccurate information. The CMPPA amended provisions originally enacted by the Privacy Act. Thus, implementation of the CMPPA operates within the Privacy Act's statutory framework. The CMPPA, like the Privacy Act, concerns *records* of U.S. citizens or permanent legal residents.[54]

What is a matching agreement and how is it used?

Matching agreements—sometimes called computer matching agreements (CMAs)—are statutorily required for agencies that conduct matching programs. The Computer Matching and Privacy Protection Act of 1988 establishes procedures for agencies when they disclose and match data on individuals for certain purposes using computers and automated records (i.e., operate a

[52] DOJ, *Overview of the Privacy Act of 1974*, p. 206.

[53] 5 U.S.C. §552a(i).

[54] *Record* is defined at 5 U.S.C. §552a(a)(4). See discussion of the definition under "What is the Privacy Act of 1974?"

"matching program").[55] The purposes contemplated by the CMPPA are for (1) determining eligibility for federal benefit programs,[56] (2) recouping payments and debts under those programs, and (3) comparing records of federal personnel. Matching agreements contain certain information about the conduct of a matching program. Within a matching program, parties are known as either the source agency[57] or the recipient agency,[58] and the matching agreement is between these parties.

There are two types of matching programs that are subject to a matching agreement. The first type is any computerized comparison of two or more automated systems of records[59] which are under the control of federal agencies, including systems of records related to federal personnel and payroll. This first type thus represents matching programs between federal agencies. The second type is any computerized comparison of a system of records with nonfederal records, which are limited to those from state or local governments and agencies thereof. The second type is thus between a federal agency and a nonfederal agency.[60]

Matching agreements are required to include certain information, including the legal authority for conducting the matching program. The CMPPA does not itself authorize any disclosures of data for matching. Matching agreements may reference a legal authority that, for example, directly implicates one of the purposes contemplated by the CMPPA, may cite an authority that provides for the disclosure of data, or may cite a routine use of the systems of records that specifies such disclosure.[61] In addition to the purpose and legal authority for conducting the matching program, matching agreements are required to include:

- the justification for the matching program and the anticipated results, including specific estimates of any savings;
- a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the anticipated start and completion dates of the matching program;
- procedures for providing individualized notice at the time of application, and notice periodically thereafter, to applicants and recipients of federal benefit program assistance and to applicants for and holders of federal personnel positions that information provided may be subject to verification through matching programs;
- procedures for verifying information produced in matching programs;
- procedures for the retention and timely destruction of identifiable records created by a recipient agency or a nonfederal agency;
- procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such matched records;

[55] 5 U.S.C. §552a(a)(8).

[56] *Federal benefit program* is defined at 5 U.S.C. §552a(a)(12).

[57] *Source agency* is defined at 5 U.S.C. §552a(a)(11).

[58] *Recipient agency* is defined at 5 U.S.C. §552a(a)(9).

[59] *System of records* is defined at 5 U.S.C. §552a(a)(5). See discussion of the definition under "What is a System of Records Notice?"

[60] 5 U.S.C. §552a(a)(10).

[61] *Routine use* is defined at 5 U.S.C. §552a(a)(7) and "means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which is was collected." For more information about routine uses, systems of records, and 5 U.S.C. §552a, see the questions and answers under "Privacy."

- prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the nonfederal agency except where required by law or essential to the conduct of the matching program;
- procedures governing the use of records from a source agency by a recipient agency or nonfederal agency, including procedures for returning records to the source agency or destroying such records;
- information on accuracy assessments of records to be used in the matching program; and
- a notice that the Comptroller General may have access to all records of a recipient agency or a nonfederal agency that the Comptroller General deems necessary to monitor or verify compliance with the agreement.[62]

Who approves a matching agreement?

Matching agreements are subject to the approval of an agency's Data Integrity Board (DIB).[63] An agency that engages in a matching program—either as a source or recipient agency—must establish a DIB.[64]

The CMPPA directs the head of the agency participating in a matching program to appoint certain senior officials within the agency to the DIB. Each DIB must include any senior official within the agency responsible for implementation of the Privacy Act and the inspector general (IG) if the agency has an IG.[65] Outside of members identified in statute, there is variation between agencies in the titles of members that comprise an agency's DIB (e.g., assistant secretary, general counsel), and in the number of members. Changes to an agency's board's membership is to be included in an annual report that is compiled by the DIB and required by the CMPPA.[66]

Once approved, and subject to a 60-day waiting period as discussed below, matching agreements are valid for an initial period of no more than 18 months.[67] Within three months of the expiration of the initial agreement, the agreement may be renewed for one additional year if the matching program will be conducted without any change.[68] After the expiration of the one-year extension, the agencies may reestablish the matching program with a new matching agreement.

What information is Congress and the public supposed to receive about matching agreements?

In OMB's Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, each agency with one or more matching programs is to list and provide links to up-to-date matching agreements for all active matching programs on the

[62] 5 U.S.C. §552a(o).

[63] 5 U.S.C. §552a(u)(3)(A). If a matching agreement is disapproved by a data integrity board, then either party to the matching agreement can appeal to the Director of the Office of Management and Budget (OMB) (5 U.S.C. §552a(u)(5)(A)).

[64] 5 U.S.C. §552a(u)(1).

[65] 5 U.S.C. §552a(u)(2).

[66] 5 U.S.C. §552a(u)(3)(D).

[67] 5 U.S.C. §552a(o)(2)(C).

[68] 5 U.S.C. §552a(o)(2)(D).

agency's Privacy Act website.[69] In practice, it is challenging to determine the number of matching programs being conducted at any given time. Although OMB directs agencies to make matching agreements available through their websites, there is no enforcement mechanism for the requirement.

Where an agency's website does not list matching programs or provide links to matching agreements, other sources of information about matching programs are available. Agencies acting as a recipient agency in a matching program must publish notice of the matching program in the *Federal Register*.[70] Agencies are required to publish these notices 30 days before conducting a new matching program or conducing a matching program that has been modified.

By statute, the Senate Homeland Security and Governmental Affairs Committee and the House Committee on Oversight and Reform are to be provided with advance notice of a matching program.[71] An agency is to report proposals for new, re-established, or significantly modified matching programs to the committees in order to permit an evaluation of the probable or potential effect of the proposal on the privacy (or other rights) of individuals.[72] OMB clarifies in *Circular No. A-108* that submitting notice of a new or significantly modified matching program to OMB and Congress occurs prior to public notice in the *Federal Register* and, furthermore, that OMB will have 30 days to review the new or modified matching program.[73] As a result, a new matching program cannot begin for at least 60 days following the approval of the matching agreement by the DIBs at the source and recipient agencies, assuming OMB or a committee does not intervene.[74]

What is not covered by matching agreements?

The CMPPA does not define matching as the activity to be regulated. Rather, the CMPPA defines what constitutes a matching program that would be subject to the act's requirements. While computer matching in general may invoke various methods and have various uses, the scope of the CMPPA is limited to what the statute has defined as a matching program, which includes the purposes of such matching. OMB, as part of its guidance interpreting the CMPPA, warns agencies against "engaging in activities intended to frustrate the normal application of the act."[75] OMB also states that it is "extremely concerned that agencies not adopt data exchange practices that

[69] Office of Management and Budget, *Circular No. A-108*, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 23, 2016, p. 30, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf.

[70] 5 U.S.C. §552a(e)(12).

[71] 5 U.S.C. §552a(r). See also *Circular No. A-108*, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 23, 2016, p. 20, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf.

[72] 5 U.S.C. §552a(r).

[73] OMB, *Circular No. A-108*, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," December 23, 2016, p. 20, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf.

[74] For example, OMB may request agencies to incorporate changes or clarifications stemming from its review. In addition, agencies may have to address comments from the public that stem from the public notice period. As such, agencies may have to delay the start of a matching program longer than the 60 days implied in statute and guidance (see Table "Illustration of Standard Review Process for Matching Programs" in OMB, *Circular No. A-108*, p. 21, https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A108/omb_circular_a-108.pdf).

[75] OMB, "Privacy Act of 1974; Final Guidance Interpreting the Provisions of P.L. 100-503, the Computer Matching and Privacy Protection Act of 1988," 54 *Federal Register* 25818, June 19, 1989.

deliberately avoid the reach of the act where compliance would otherwise be required."[76] While the statutory definition of "matching program" includes the words "any computerized comparison," the absence of a description of methods that meet the definition permits agencies to derive their own interpretations of what types of matching methods are covered by the CMPPA. The result is that some agencies' activities may potentially avoid the coverage by the CMPPA.

The CMPPA explicitly excepts some matching from the definition of matching programs.[77] Matches that are excepted may be arranged into six different categories. Broadly, these categories include (1) for research and statistics; (2) matching with no adverse impact to federal employees; (3) for law enforcement, security, and intelligence; (4) for the administration of taxes, levies, and certain savings programs; (5) for inspectors general and with respect to fraud, waste, and abuse; and (6) selected matches by the Social Security Administration involving incarcerated and other justice-system-involved individuals.

Federal Records

The Federal Records Act (FRA; P.L. 81-754), enacted in 1950 and amended since, governs the collection, retention, and preservation of federal agency records. Congress deemed federal records worthy of preservation for the information they provide on the transaction of public business and also because they document the "organization, functions, policies, decisions, procedures, and essential transactions" of the government.[78] The National Archives and Records Administration (NARA), headed by the Archivist of the United States, oversees the implementation of the FRA and agency records management programs.

What is a federal record?

The FRA provides a definition of federal records in order to determine whether particular recorded information should be retained and managed. Whether or not materials meet the definition of federal record is based on an assessment of the content of the information and not the format on which the information is stored. The definition of "federal record" for the purposes of the FRA is separate and distinct from the definition of "record" under the Privacy Act.

Federal records include

> 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.[79]

The definition excludes library and museum materials made for reference or exhibition purposes and duplicate copies of records preserved only for convenience.

In cases where there is disagreement over whether particular recorded information constitutes a federal record, statute expressly empowers the Archivist to determine "whether recorded information, regardless of whether it exists in physical, digital, or electronic form, is a record" for

[76] Ibid.

[77] 5 U.S.C. §552a(a)(8)(B).

[78] 44 U.S.C. §3301.

[79] Ibid.

purposes of the FRA and states that this determination "shall be binding on all Federal agencies."[80]

How long must federal records be kept?

A records schedule is created by agencies in consultation with NARA and provides a disposition authority for the set of records discussed in the schedule. The disposition authority provides information on where the information should be stored and if and when the information should be destroyed.

A records schedule can be any of the following:

- a standardized form (SF 115) that has been approved by NARA to authorize the disposition of federal records (i.e., disposition authority);[81]
- a General Records Schedule (GRS) issued by NARA, which authorizes, after specified periods of time, the destruction of temporary records or the transfer of permanent records to the Archives that are common to several or all agencies;[82] or
- a published agency manual or directive containing the records descriptions and disposition instructions approved by NARA on one or more standardized forms or issued by NARA in the GRS.

All federal records must be covered by a NARA-approved records schedule or a GRS.

The records schedule should include a description of each type or series of records and note whether the records are temporary (to be discarded by the federal government) or permanent (to be permanently retained by NARA). For permanent records, the schedule includes the date the record would be transferred to NARA.

Records schedules must be cleared by internal agency stakeholders, the Government Accountability Office when required by 43 C.F.R. Section 1225.20(a), and by NARA. Disposition instructions approved by NARA are mandatory.[83] In addition, NARA must publish a notice of agency requests for the disposal of records in the *Federal Register*.[84] If NARA has previously approved a request to dispose of the records covered in an agency request, a notice is published only if the proposed retention period is shorter. The publication of these notices allows interested persons to submit written comments on the records to NARA before disposal is approved or reapproved with a shorter retention period.

Are there penalties for violating the Federal Records Act?

In the event of unlawful removal, defacing, or erasure of records, the FRA requires the Archivist to initiate action through the Attorney General for the recovery of the records.[85] Specifically:

> In any case in which the head of a Federal agency does not initiate an action for such recovery or other redress within a reasonable period of time after being notified of any such

[80] 44 U.S.C. §3301(b).

[81] A copy of SF 115 may be located at NARA, *Standard Form (SF) 115*, https://www.archives.gov/records-mgmt/policy/standard-form-115.html.

[82] See also NARA, *What Are the General Records Schedules (GRS)*, https://www.archives.gov/records-mgmt/grs.

[83] 44 U.S.C. §3314.

[84] 44 U.S.C. Section 3303a(a).

[85] 44 U.S.C. §3106.

> unlawful action described in subsection (a), or is participating in, or believed to be participating in any such unlawful action, the Archivist shall request the Attorney General to initiate such an action, and shall notify the Congress when such a request has been made.[86]

Thus, investigation of the unlawful removal or destruction of government and presidential records requires the joint cooperation of NARA and the Department of Justice (DOJ). The Archivist may not independently initiate action without the Attorney General. NARA provides information on missing records and efforts to retrieve materials online.

Section 2071 of Title 18 of the U.S. Code states that a person who is found guilty of "willfully and unlawfully" concealing, removing, mutilating, obliterating, destroying, or attempting to do any such action against a record can be fined and imprisoned for up to three years.[87] It further provides that anyone holding federal office who is convicted of this crime with respect to records in his or her custody, in addition to fines and possible imprisonment, can lose his or her position and be disqualified from holding federal office in the future.[88]

Additional Questions

Who may I contact with additional questions related to this report?

If you have questions related to one of the topics covered in this report, you may reach out to the analysts listed below:

- **IT Management** – Dom Fiorentino
- **Cybersecurity** – Chris Jaikaran
- **Privacy** – Meghan Stuessy
- **Federal Data Integration** – Natalie Ortiz
- **Federal Records** – Meghan Stuessy

Who may I contact if I have a question that was not answered in this report?

If you have additional questions, please use the "Place A Request" button on crs.gov or call 7-5700 to place a request.

[86] Ibid.

[87] 18 U.S.C. §2071.

[88] Ibid.

Appendix. Additional Resources

This appendix provides references to additional CRS reports pertaining to the subjects covered here, in alphabetical order by topic.

Congressional Oversight

- CRS Report RL30240, *Congressional Oversight Manual*, coordinated by Ben Wilhelm, Todd Garvey, and Christopher M. Davis
- CRS In Focus IF10015, *Congressional Oversight and Investigations*, by Todd Garvey, Mark J. Oleszek, and Ben Wilhelm
- CRS Report R41079, *Congressional Oversight: An Overview*, by Walter J. Oleszek

Cybersecurity

- CRS In Focus IF10559, *Cybersecurity: A Primer*, by Chris Jaikaran
- CRS In Focus IF12851, *Legislating on Cybersecurity*, by Chris Jaikaran
- CRS Report R46926, *Federal Cybersecurity: Background and Issues for Congress*, by Chris Jaikaran
- CRS Insight IN12142, *HSA@20 Episode Companion: Cybersecurity*, coordinated by William L. Painter

Federal Data Integration

- CRS Report R47325, *Computer Matching and Privacy Protection Act: Data Integration and Individual Rights*, by Natalie R. Ortiz
- CRS In Focus IF12334, *Preventing Improper Payments: Lessons from Using Data Matching in Pandemic Relief Program Oversight*, by Natalie R. Ortiz and Ben Wilhelm
- CRS Report R48053, *Federal Data Management: Issues and Challenges in the Use of Data Standards*, by Natalie R. Ortiz

Federal Records

- CRS Report R43072, *Common Questions About Federal Records and Related Agency Requirements*, by Meghan M. Stuessy
- CRS In Focus IF11119, *Federal Records: Types and Treatments*, by Meghan M. Stuessy
- CRS In Focus IF11220, *Electronic Messaging Recordkeeping Requirements*, by Meghan M. Stuessy
- CRS In Focus IF12432, *Managing Electronic Messages from High-Level Officials Through Capstone*, by Meghan M. Stuessy

IT Management

- CRS Report R48147, *Chief Information Officers (CIOs): Agency Roles and Responsibilities*, by Meghan M. Stuessy and Dominick A. Fiorentino
- CRS Report R46877, *Federal Information Technology (IT) Budgeting Process in the Executive Branch: An Overview*, by Dominick A. Fiorentino

- CRS Report R42826, *The Federal Acquisition Regulation (FAR): Answers to Frequently Asked Questions*, by David H. Carpenter, Matthew D. Trout, and Dominick A. Fiorentino
- CRS Report R42826, *The Federal Acquisition Regulation (FAR): Answers to Frequently Asked Questions*, by David H. Carpenter, Matthew D. Trout, and Dominick A. Fiorentino

The Privacy Act

- CRS Report R47058, *Access to Government Information: An Overview*, by Meghan M. Stuessy
- CRS Report R47863, *The Privacy Act of 1974: Overview and Issues for Congress*, by Meghan M. Stuessy

Author Information

Chris Jaikaran, Coordinator
Specialist in Cybersecurity Policy

Natalie R. Ortiz
Analyst in Government Organization and Management

Dominick A. Fiorentino
Analyst in Government Organization and Management

Meghan M. Stuessy
Analyst in Government Organization and Management

Disclaimer