

FEDERAL COMMUNICATIONS COMMISSION Washington, D.C. 20554 FCC DIRECTIVE	TITLE	
	FCC Privacy Act Manual	
	Directive Number: FCCINST 1113.1	Effective Date: March 2016

TO: All Employees.

SUBJECT: FCC Privacy Act Manual

Purpose. To transmit the Federal Communications Commission (“FCC” or “Commission”) Privacy Act Manual, setting forth the authorities, objectives, responsibilities, and procedures for the program to implement the *Privacy Act of 1974*, as amended, (“Privacy Act” or “Act”) within the FCC. It supplements the requirements and procedures of FCC Privacy Act Regulations, 47 CFR Sections 0.551 – 0.561.

Scope. This Directive applies to all employees, interns, and consultants, and is also applicable to contractors as a term of their contract with the FCC.

Authority. *Privacy Act of 1974*, as amended, 5 U.S.C. 552a; *Federal Information Security Modernization Act of 2014*, XXXX; Section 208 of the E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. 3541, *et seq.*; *Computer Matching and Privacy Protection Act of 1988*, Pub. L. 100-503, *et seq.*;

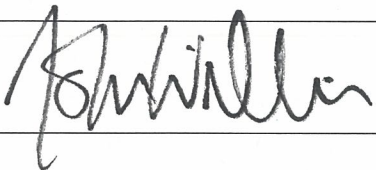
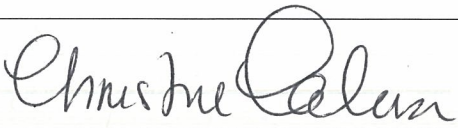

Office of Management and Budget (OMB) Circulars and Memoranda, as listed and updated at: http://www.whitehouse.gov/omb/inforeg_infopolitech#pg; National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (as listed and updated at: <http://csrc.nist.gov/publicationss/>); CIO Council, *Privacy Best Practices for Social Media*, July 2013; *Federal Register Document Drafting Handbook*, (“Document Drafting Handbook”) National Archives and Records Administration (NARA), Office of the Federal Register, October 1998 Revision; and “Initial Privacy Assessment (IPA), Instructions and Template.” Department of Justice (DOJ), Office of Privacy and Civil Liberties, March 2010 Revision.

Policy and Objective. An individual’s privacy is a right that must be respected and protected. It is the policy of the FCC that all employees and contractors shall be made aware of, and comply with, the Privacy Act, and all applicable laws and guidelines addressing privacy, and that information about individuals shall be collected, maintained, used, disseminated, protected, and disposed of (when no longer needed or out-of-date), in accordance with the Privacy Act and FCC regulations and policy. The objective in developing the FCC Privacy Act Manual is to make available to employees and contractors in a single publication basic information about their rights, duties, and responsibilities under the Privacy Act and the Commission policies, procedures, and information requirements for implementing the Act.

Cancellation. This instrument supersedes FCCINST 1113.1, dated August 1, 2005.

Location. FCC Privacy Act webpage: <https://www.fcc.gov/sites/default/files/fcc-privacy-act-manual.pdf>.

RECORD OF APPROVAL

Title: Senior Agency Official for Privacy (SAOP)	
Printed Name: John B. Williams	
Signature: 	Date: 9/24/18
Title: Chief Information Officer (CIO)	
Printed Name: M. Christine Calvosa	
Signature: 	Date: 24 sept 2018
Title: Privacy Manager (PM)	
Printed Name: Leslie F. Smith	
Signature: 	Date: 09/24/2018

REVISION LOG

Date:	Description:	Author:

FCC PRIVACY ACT MANUAL – FCCINST 1113.1

TABLE OF CONTENTS

CHAPTERS

CHAPTER 1	FCC PRIVACY POLICIES AND GENERAL PROVISIONS
CHAPTER 2	COLLECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)
CHAPTER 3	DISCLOSING PERSONALLY IDENTIFIABLE INFORMATION (PII) IN RECORDS
CHAPTER 4	ACCESS, AMENDMENT, AND APPEALS BY INDIVIDUALS
CHAPTER 5	PRIVACY ACT EXEMPTIONS
CHAPTER 6	NEW, REVISED, OR CANCELLED SYSTEMS OF RECORDS
CHAPTER 7	EMPLOYEE PERFORMANCE RECORDS MAINTAINED BY SUPERVISORS
CHAPTER 8	INFORMATION SYSTEMS AND TECHNOLOGY GUIDELINES
CHAPTER 9	PRIVACY IMPACT ASSESSMENTS (PIA)
CHAPTER 10	COMPUTER MATCHING PROGRAM GUIDELINES
CHAPTER 11	DATA INTEGRITY BOARD
CHAPTER 12	FEDERAL AGENCY WEBSITES PRIVACY POLICIES
CHAPTER 13	THIRD PARTY WEBSITES AND APPLICATIONS
CHAPTER 14	PRIVACY TRAINING
CHAPTER 15	<i>FEDERAL INFORMATION SECURITY AND MANAGEMENT ACT (FISMA) PRIVACY REQUIREMENTS</i>
CHAPTER 16	FCC PRIVACY BREACH NOTIFICATION POLICY

APPENDICES

APPENDIX 1	GUIDELINES FOR PROTECTING SSNS AND PII
APPENDIX 2	OFFICE OF FEDERAL REGISTRAR SORN TEMPLATE
APPENDIX 3	ADAPTED PRIVACY IMPACT ASSESSMENT (PIA) TEMPLATE
APPENDIX 4	OMB GUIDANCE ON THE ADAPTED PIA TEMPLATE
APPENDIX 5	FCC WEBSITE PRIVACY POSTING REQUIREMENTS
APPENDIX 6	SAOP ANNUAL FISMA PRIVACY REPORT

APPENDIX 7 OFFICE OF FEDERAL REGISTRAR MATCHING ACTIVITIES TEMPLATE
APPENDIX 8 MATCHING ACTIVITIES CHECKLIST
APPENDIX 9 FISMA BUREAU/OFFICE/DIVISION REPORTING QUESTIONNAIRE

CHAPTER 1

GENERAL PROVISIONS

- 1-1. Purpose. This directive sets forth the policies, authorities, objectives, responsibilities, and procedures for the Federal Communications Commission (FCC or Commission or agency) to implement the Commission's privacy program as required by the *Privacy Act of 1974*, as amended, 5 U.S.C. 552a, supplemented by Congressional statutes, and the directives and policy guidance on privacy issued by the Office of Management and Budget (OMB). This manual also supplements the requirements and procedures of the FCC Privacy Act Regulations, 47 CFR §§ 0.551–0.561.
- 1-2. Background.
- (A) The primary objective of the *Privacy Act of 1974*, as amended, (the “Act”) is to achieve an appropriate balance between the Federal Government's need for information about individuals and each individual's right to privacy.
 - (B) The Act seeks to achieve this objective through procedures to regulate the collection, maintenance, use, dissemination, retention, and disposal of personally identifiable information (PII) by the FCC and other Federal agencies.
 - (C) The Act also establishes a system of checks and balances to assure effective operation of these procedures. These checks and balances include provisions for the exercise of individual rights, public scrutiny of agency recordkeeping practices, Office of Management and Budget (OMB) and Congressional oversight of Federal agency activities, and both civil and criminal sanctions.
 - (D) The Privacy Act establishes a number of basic rights of individuals who are the subject of Federal recordkeeping. It gives individuals:
 - (1) The right to know the **authority** (whether granted by statute or by Executive Order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary.¹
 - (2) The **principal purpose(s)** for which the information is intended to be used.²
 - (3) The **routine uses** which may be made of the information, as published pursuant to 5 U.S.C. 552a(e)(4)(D) of the Privacy Act.³
 - (4) The **effects** on the individual, if any, of not providing all or any part of the requested information.⁴

¹ 5 U.S.C. 552a(e)(3)(A).

² 5 U.S.C. 552a(e)(3)(B).

³ 5 U.S.C. 552a(e)(3)(C).

⁴ 5 U.S.C. 552a(e)(3)(D).

- (5) The **right of access** to Commission records about them, and to Commission records of the disclosure of this information.⁵
- (6) The **right to request amendment, correction, or expungement** of records about them.⁶
- (7) The **right to appeal** an adverse decision regarding amendment of records to a higher authority in the Commission.⁷
- (8) The **right to sue** an agency in U.S. District Court to gain access to or amendment of records, or to obtain damages for violation of the Privacy Act which result in an injury to the individual subject.⁸

1-3. Authorities.

- (A) 47 CFR §§ 0.551-0.561. (“FCC Privacy Act Regulations”).
- (B) CIO Council, *Privacy Best Practices for Social Media*, July 2013.
- (C) Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act*, Executive Office of the President (EOP), Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA), December 2015 (Draft).
- (D) Circular No. A-130 (Revised), *Management of Federal Information Resources*, EOP, OMB, OIRA, 1999.
- (E) *Computer Matching and Privacy Protection Act of 1988* (“Computer Matching Act”) (Public Law 100-503).
- (F) *E-Government Act of 2002* (Public Law 107-347), 44 U.S.C. Ch. 36.
- (G) *Federal Register Document Drafting Handbook*, (“Document Drafting Handbook”) National Archives and Records Administration (NARA), Office of the Federal Register, October 1998 Revision.
- (H) *Final Guidance for Conducting Matching Programs*, OMB (54 FR 25819) June 19, 1989.
- (I) *Guidance for Conducting Matching Programs*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs (47 FR 21656-21658) May 19, 1982.

⁵ 5 U.S.C. 552a(d)(1), and 552a(e)(4)(H); 47 CFR §§ 0.554(a), 0.555(a), 0.555(b), and 0.558.

⁶ 5 U.S.C. 552a(d)(2); 47 CFR §§ 0.556, 0.557, and 0.558.

⁷ 5 U.S.C. 552a(d)(3); 47 CFR §§ 0.555(e), 0.556(c)(2), and 0.557.

⁸ 5 U.S.C. 552a(g); 47 CFR §§ 0.555(e)(2) and 0.557(d)(4).

- (J) “Initial Privacy Assessment (IPA), Instructions and Template.” Department of Justice (DOJ), Office of Privacy and Civil Liberties, March 2010 Revision.
- (K) *Memorandum for the Senior Officials for Information Resources Management*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, May 24, 1985.
- (L) Memorandum M-99-18, *Guidance and Model Language for Federal Web Site Privacy Policies*, EOP, OMB, OIRA, June 1, 1999.
- (M) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, EOP, OMB, OIRA, September 26, 2003.
- (N) Memorandum M-05-04, *Policies for Federal Agency Public Websites*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, Office of Management and Budget, December 17, 2004.
- (O) Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, February 11, 2005.
- (P) Memorandum M-06-16, *Protection of Sensitive Agency information*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, June 23, 2006.
- (Q) Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, Executive Office of the President, Office of Management and Budget, Office of E-Government and Information Technology, July 12, 2006.
- (R) Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, June 25, 2010.
- (S) Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, June 25, 2010.
- (T) Memorandum M-11-02, *Sharing Data While Protecting Privacy*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs, November 3, 2010.
- (U) Memorandum, June 18, 2007, *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft*, U.S. Office of Personnel Management.
- (V) *Overview of the Privacy Act of 1974*, “Definitions,” Department of Justice (DOJ), May 2000 ed., www.doj.gov.
- (W) *Privacy Act of 1974*, as amended (Public Law 93-579, 5 U.S.C. 552a).

- (X) *Privacy Act Guidelines*, Executive Office of the President, Office of Management and Budget, Office of Information and Regulatory Affairs (40 FR 28949-28978) July 9, 1975.
- (Y) “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” FCC Memorandum, September 22, 2007.

1-4. **Definitions.** For the purposes of this directive, the following definitions shall apply:

- (A) **Access Request** means a request by an individual or authorized representative to see or receive a copy of a record in a particular system of records of which he/she is the subject. The request must show dependence on the Privacy Act.⁹ This is also called a **Privacy Request**.
- (B) **Agency** includes any executive or military department, Government corporation, Government controlled corporation, or other establishment of the executive branch of the Federal Government, or any independent regulatory agency such as the FCC.¹⁰
- (C) **Disclosure** means giving information contained in a system of records, by any means, to any person other than the individual to whom the record pertains, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record (or information) pertains. This includes the transfer or divulging of a record to another agency.¹¹
- (D) **Individual** means a “citizen of the United States” or an “alien lawfully admitted for permanent residence.”¹²
 - (1) The parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.¹³
 - (2) The deceased, nonresident aliens, corporations and organizations, and third parties have no rights under the Privacy Act.¹⁴
- (E) **Information in Identifiable Form** is any information or data in an electronic database or information technology system, such as FCC forms or in an online data collection on the Internet, that:

⁹ 5 U.S.C. 552a(d)(1); 47 CFR § 0.554(a).

¹⁰ 5 U.S.C. 552a(a); 552a(e); OMB Circular A-130, *Memorandum for Heads of Executive Departments and Agencies: Management of Federal Resources*, at 6(a); 47 CFR § 0.551(a).

¹¹ 5 U.S.C. 552a(b).

¹² 5 U.S.C. 552a(a)(2); 47 CFR § 0.551(b)(1); OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions for the E-Government Act of 2002*, EOP, OMB, OIRA, September 26, 2003, at 2.

¹³ 5 U.S.C. 552a(h).

¹⁴ DOJ, *Overview of the Privacy Act of 1974*, “Definitions,” at B, “Individual, comment--“ May 2000 ed., www.usdoj.gov.

- (1) Directly identifies an individual, such as his/her name, address, Social Security Number, or other identifying number or code, telephone number, e-mail address, photographs, and voice prints; and/or
 - (2) The FCC (or other Federal agency) uses to identify specific individuals in conjunction with other data elements, *i.e.*, indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, or other descriptive elements.)¹⁵
- (F) **Information System** is any process of collection, maintenance, use, or dissemination of information, whether performed manually with paper records, documents, and files, or electronically through the use of information technology (IT) products or design.¹⁶
- (G) **Information Technology (IT)** means any equipment, software, or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.¹⁷
- (H) **Maintain** means to maintain, collect, use, or disseminate records.¹⁸
- (I) **Personally Identifiable Information (PII)** means any information about an individual maintained by a Federal agency, including but not limited to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.¹⁹
- (1) The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.²⁰
 - (2) In trying to assess whether information should be labeled as PII, it is important for Commission staff and contractors to recognize that non-PII can become PII whenever additional information is made publicly available—in any medium

¹⁵ OMB Memorandum M-03-22 (September 26, 2003), "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," at 3.

¹⁶ USDOJ, OPCL, "Initial Privacy Assessment (IPA) Instructions & Template," (Revised March 2010), at 1.

¹⁷ OMB Memorandum M-03-22 (September 26, 2003), "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," at 3; U.S. Department of Homeland Security, Privacy Office, "Privacy Threshold Analysis (PTA) (June 10, 2010), at 2 (footnotes); 40 U.S.C. 11101(6);

¹⁸ 5 U.S.C. 552a(a)(3).

¹⁹ OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," at foot note 1; FCC Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 22, 2007, at 2.

²⁰ OMB Memorandum M-10-23 (June 25, 2010), "Guidance for Agency Use of Third-Party Websites and Applications," at 8.

and from any source—that, when combined with other available information, could be used to identify an individual.²¹

- (3) The FCC may make PII available by any Commission action that causes PII to become available or accessible to the FCC, whether or not the Commission solicits it or collects it.²²
 - (a) In general, an individual can make PII available to the FCC (or another Federal agency) when he or she provides, submits, communicates, links, posts, or associates PII while using the website or applications.²³
 - (b) This is particularly true with the advent of third-party websites or other such applications or social media, which are outside the FCC’s jurisdiction and control, and thus may pose additional risks of inadvertent disclosure of PII.
 - (c) “Associate” can become activities commonly referred to as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions.”²⁴

The issues concerning PII in “social media” are explained fully in **Chapter 13**.

- (J) **Record** means any item, collection, or grouping of information about an individual that is maintained by the Commission, including, but not limited to, his/her education, financial transactions, medical history, and criminal or employment history, and that contains his/her name, or the identifying number, symbol, or other identifying particular assigned to an individual, such as a finger or voice print, or photograph.²⁵

A record in a system of records must contain **two elements: a personal identifier** and at least **one item of personal information**.²⁶

- (K) **Routine Use** means, with respect to disclosure of a record outside the Commission, the use of such record for a purpose, which is compatible with the purpose for which the record was collected.²⁷

The term encompasses not only common and ordinary uses, but also all proper and necessary uses, even if they are infrequent. Routine uses must be shown in the system(s) notice, which is published in the *Federal Register*.²⁸

²¹ OMB Memorandum M-10-23, at 8.

²² OMB Memorandum M-10-23, at 8.

²³ OMB Memorandum M-10-23, at 8.

²⁴ OMB Memorandum M-10-23, at 8.

²⁵ 5 U.S.C. 552a(a)(4); 47 CFR § 0.551(b)(2); OMB Circular A-130, at 6(w).

²⁶ 5 U.S.C. 552a(a)(4); 47 CFR § 0.551(b)(2).

²⁷ 5 U.S.C. 552a(a)(7); 47 CFR § 0.551(b)(4).

²⁸ 5 U.S.C. 552a(e)(3)(c) and 552a(e)(4)(D); 47 CFR §§ 0.552(d) and 0.553(d).

(L) **System of Records** means any group of records, including but not limited to information in paper documents and files and electronic files, records, and data, under the control of the FCC (or other Federal 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,²⁹ *e.g.*, a name or Social Security Number (SSN):

- (1) A file or grouping of records that is arranged chronologically, or by subject or other means, and which is not retrieved by an individual identifier, is not a system of records under the Act.
- (2) If retrieval by individual identifier is possible but not actually done, or if it depends on memory, the group is not a system of records.
- (3) However, creating a retrieval system or cross-index, arranged by personal identifier, for records that are filed randomly or by non-personal symbols makes that collection a system of records.³⁰

(M) **System of Records Notice (SORN)** means the notice that is published in the *Federal Register* as required by 5 U.S.C. 552a(e)(4) of the Privacy Act.³¹

A notice, *i.e.*, SORN, must be published in the *Federal Register* to describe a new or altered system of records, as required by OMB Circular A-108.³²

(N) **System Manager** means the Commission official responsible for the storage, maintenance, safekeeping, and disposal of a system of records.³³

The system manager does not have to have physical custody of the records; however, he/she must be able to exercise effective controls for operating and safeguarding the system.³⁴

1-5. **Policies and Objectives.** It is the FCC's policy that an individual's privacy is a right that must be respected and protected and that all Commission employees and contractors shall be made aware of, and comply with, the requirements of the Privacy Act, and other applicable laws and guidelines addressing privacy and information related to an individual, *i.e.*, personally identifiable information (PII). In order to protect each individual's privacy, the Commission will:

- (A) Implement the *Privacy Act of 1974*, 5 U.S.C. 552a, as amended, Congressional statutes and OMB guidance on privacy, and protect the rights of individuals in the accuracy and privacy of information, *i.e.*, personally identifiable information (PII), concerning him/her which is contained in Commission records.³⁵

²⁹ 5 U.S.C. 552a(a)(5); 47 CFR § 0.551(b)(3).

³⁰ DOJ, *Overview of the Privacy Act of 1974*, "Definitions," at E, "System of Records, comment-- May 2000 ed., www.usdoj.gov.

³¹ 5 U.S.C. 552a(e)(4); 47 CFR § 0.552.

³² OMB Circular A-108, at 5ff.

³³ 47 CFR § 0.551(b)(5).

³⁴ 5 U.S.C. 552a(e)(4)(F), 552a(e)(9), and 552a(e)(10); 47 CFR §§ 0.552(f), 0.554(c), 0.555(a)(1), 0.555(b)(1), 0.556(a), 0.556(c), and 0.556(d).

³⁵ 47 CFR §§ 0.551(a) and 555(b); 5 U.S.C. 552a(b) and 552a(e).

- (B) Collect, maintain, and use information in systems of records only in support of programs authorized by law or executive order of the President.³⁶
- (C) Amend, upon the individual's request, any record that does not meet these standards noted above, as part of the Commission's commitment to accuracy, completeness, and accountability.³⁷
- (D) Review the current holdings of all PII, on a regular schedule and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of documented Commission functions.³⁸
- (E) Continue the Commission's on-going efforts, consistent with Federal regulations and OMB guidelines:
 - (1) To eliminate any unnecessary uses of Social Security Numbers (SSNs) and to limit their use to only those instances where the SSN is required by statute or another party, such as conformance with the Debt Collection Improvement Act or meeting the requirements of other Federal agencies like the Office of Personnel Management (OPM), Internal Revenue Service (IRS), General Services Administration (GSA), Government Accountability Office (GAO), Department of Homeland Security (DHS), law enforcement, or court requirements;³⁹
 - (2) To work with other Federal agencies and external parties, including OPM and the National Finance Center (NFC), to reduce or eliminate the use of SSNs;⁴⁰ and
 - (3) To strengthen the protection of PII, including SSNs, from theft or loss.⁴¹
- (F) Conduct an annual review and update of the FCC's systems of records identified on the FCC Privacy Act webpage: at <https://www.fcc.gov/general/privacy-act-information#systems> to ensure that the PII in these systems conforms to the four criteria listed above. This review requirement is part of the FCC's annual preparations for the privacy section of the annual FISMA submission to OMB.⁴²

³⁶ 5 U.S.C. 552a(e)(1).

³⁷ 5 U.S.C. 552a(d)(2) and 552a(e)(6); 47 CFR § 0.556.

³⁸ OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), at 6; 5 U.S.C. 552a(e)(5) and 552a(e)(6); 47 CFR § 0.556.

³⁹ OMD Memorandum M-07-16, at 18.

⁴⁰ OMD Memorandum M-07-16, at 19.

⁴¹ OMD Memorandum M-07-16, at 19; Memorandum, June 18, 2007, "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft, U.S. Office of Personnel Management, at 1. **CHECK**

⁴² OMD Memorandum M-07-16, at 19; 5 U.S.C. 552a(d)(2) and 552a(e)(6); 47 CFR § 0.556.

- (G) Permit an individual to know about, review, and have copies of agency records pertaining to him/her,⁴³ except where they are covered by a published exemption from such disclosure, or where created in anticipation of a civil action or proceeding.⁴⁴
- (H) Amend, upon the individual's request and with the Commission's concurrence, any record that does not meet these standards, as noted above, and as part of the Commission's commitment to accuracy, completeness, and accountability.⁴⁵
- (I) Establish appropriate administrative, technical, and physical "safeguards" to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity, *e.g.*, data breaches, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.⁴⁶
- (I) Participate, whenever practicable, in Federal inter-agency high-value data sharing arrangements that support important FCC, Executive Branch, and Congressional initiatives, inform public policy decisions, and improve program implementation while simultaneously embracing responsible Federal stewardship. In such data sharing arrangements, it is the FCC's policy to protect each individual's privacy (*i.e.*, safeguarding PII) by complying with the Privacy Act and all other applicable privacy laws, regulations, and policies.⁴⁷
- (J) Conduct a review of how PII is handled within the FCC when the Commission uses information technology (IT) to collect new information, or when the Commission develops or buys new IT systems to handle collections of PII⁴⁸ consistent with Federal statutes and regulations and OMB requirements.
- (K) Report any real or suspected breach of PII to the appropriate Federal authorities, as required by Executive Order 13402 and the Commission's breach notification policy.⁴⁹

Note: This policy is explained in more detail in Chapter X, FCC's Breach Notification Policy on the FCC Privacy Act Webpage at: [\[insert link\]](#)

- (L) Establish "Rules of Conduct:"
 - (1) For all persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of the Privacy Act, including any other rules and procedures that have been adopted pursuant to the Act and the penalties for noncompliance.⁵⁰

⁴³ 5 U.S.C. 552a(d)(1), 552a(f)(3), 552a(j), and 552a(k); 47 CFR § 0.555.

⁴⁴ 5 U.S.C. 552a552a(d)(5); 47 CFR § 0.555.

⁴⁵ OMB Memorandum M-07-16, at 6.

⁴⁶ OMB Memorandum M-07-16, at 4; 5 U.S.C. 552a(e)(10).

⁴⁷ OMB Memorandum M-11-02, at 1.

⁴⁸ OMB Memorandum M-07-16, at 4.

⁴⁹ OMB Memorandum M-07-16, at 1.

⁵⁰ 5 U.S.C. 552a(e)(9); OMB Memorandum M-07-16, at 4;

- (2) When PII is being physically removed; and
- (3) When PII is being accessed remotely.

Note: The “rules of conduct” and security safeguards should be consistent with the protocols established by the National Institute of Standards and Technology (NIST) for FCC employees and contractors whenever PII that is being transported and/or stored outside of the FCC’s headquarters and other facilities or that is to be accessed remotely.⁵¹

- (M) Provide for review of a decision to deny an individual’s request for access to, or amendment of, records of which he/she is a subject.⁵²
- (N) Keep records for the minimum time required to protect the rights and provide for the needs of the individual and the U.S. Government. This includes permitting individuals to review the accounting of disclosures made of their records,⁵³ except in those instances where such disclosure is exempt under 47 CFR § 0.561 of FCC rules.⁵⁴
- (O) When sharing data with other Federal agencies, FCC bureaus and office are reminded that they should do so in a way that fully protects individual privacy, *i.e.*, comply with the Privacy Act and all other applicable privacy laws, regulations, and policies. In addition to the legal framework that governs the use and disclosure of data, bureaus and offices are urged to consult established codes of Fair Information Practices.⁵⁵

1-6. Responsibilities. The **Managing Director** has supervisory responsibility for the administration and management of the Privacy Act by the FCC’s senior privacy staff. In this capacity, the Managing Director has authority within the FCC to consider information privacy policy issues at the national and Commission-wide levels.

- (A) The **Managing Director** or his/her delegate shall:
 - (1) Oversee the management of the Commission’s privacy program.
 - (2) Designate a senior official (at the Assistant Secretary or equivalent level) as the FCC’s **Senior Agency Office for Privacy**, as required by OMB regulations.⁵⁶ The SAOP has agency-wide responsibility for information privacy issues, to ensure on-going compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.
- (B) The **Senior Agency Official for Privacy (SAOP)** shall:

⁵¹ OMB Memorandum M-06-16, at Action Item 2.2.

⁵² 5 U.S.C. 552a(d)(3) and 552a(f)(4); 47 CFR §§ 0.555(e)(1) and 0.557(b).

⁵³ 5 U.S.C. 552a(c).

⁵⁴ 47 CFR §§ 0.555(b) and 0.561.

⁵⁵ OMB Memorandum M-11-02, “Sharing Data While Protecting Privacy,” at 1.

⁵⁶ OMB Memorandum M-05-08, Feb. 11, 2005, “Designation of Senior Agency Official for Privacy,” at 1.

- (1) Ensure the implementation of all information privacy protections, including the Commission's full compliance with Federal laws, regulations, policies, and activities relating to privacy and privacy protections provided in these laws and regulations;⁵⁷
- (2) Have a central policy-making role in overseeing, coordinating, and facilitating the Commission's privacy compliance efforts, including the Commission's development and evaluation of legislative, regulatory, and other policy proposals that implicate information privacy issues, including comments under OMB Circular A-19;⁵⁸
- (3) Participate in assessing the impact of the Commission's use of technology on privacy and the protection of PII, such as during the development of new or significantly changed information systems and during promulgation of homeland security regulations;⁵⁹
- (4) Conduct periodic reviews of the agency's privacy procedures to insure that they are comprehensive and up-to-date (including the annual review as required under FISMA) to identify deficiencies, weaknesses, or risks in these privacy policies and programs;⁶⁰
- (5) Ensure that the Commission maintains appropriate documentation regarding compliance with information privacy laws, regulations, requirements, and policies;⁶¹
- (6) Advise the Managing Director on how the Commission's employees, contractors, and routine activities adhere to the requirements of the Privacy Act;
- (7) Work with the Commission's bureaus and offices (B/Os) to insure that they are cognizant of any privacy issues in the context of their rulemakings, regulatory, enforcement, and related activities;⁶²
- (8) Chair the Commission's Data Integrity Board that oversees information sharing, computer matching, and related issues;⁶³
- (9) Coordinate the Agency Response Team (ART) to investigate all potential, suspected, or actual data breaches and to report their findings to the US Computer Emergency Readiness Team (US-CERT);⁶⁴

⁵⁷ FCC Memorandum, "FCC Breach Notification Policy" – Revision 3, October 2010, at 2; OMB Memorandum M-05-08 (Feb. 11, 2008), "Designation of Senior Agency Official for Privacy," at 1.

⁵⁸ OMB Memorandum M-05-08, at 2; FISMA SAOP reporting guidelines, at 3b.

⁵⁹ OMB Memorandum M-05-08, at 2; FISMA SAOP reporting guidelines, at 3a, 3b, and 3c.

⁶⁰ OMB Memorandum M-05-08, at 1-2.

⁶¹ OMB Memorandum M-05-08, at 1; 2011 FISMA Report, "privacy section," 3a.

⁶² OMB Memorandum M-05-08, at 2.

⁶³ 2011 FISMA Report, "privacy section," 3b.

⁶⁴ FCC Breach Notification Policy, at 2 and 3; FCC Memorandum – Revision 3, Oct. 2010, at 2.

- (10) Review and approve all Systems of Records Notices (SORN), Privacy Threshold Analyses (PTAs), and Privacy Impact Assessments (PIAs);⁶⁵ and
 - (11) Oversee the Commission's privacy training and education programs regarding privacy laws, regulations, policies, and procedures that govern the handling of PII by employees and contractors to ensure that they receive the appropriate training and education commensurate with their duties and responsibilities.⁶⁶
- (C) The **Chief Information Officer (CIO)** or his/her delegate shall:
- (1) Preserve and protect PII contained in the FCC's systems of records;
 - (2) Audit compliance with the requirements of the Commission's privacy directives and any related internal policies and procedures;
 - (3) Establish an internal FCC Data Integrity Board that shall oversee and approve use of computer matching programs and data sharing arrangements;
 - (4) Establish training programs for FCC personnel and contractors to ensure ongoing compliance with privacy laws, regulations, policies, and procedures for handling PII;
 - (5) Designate an employee FCC Information Technology (FCC IT) manager of the FCC's privacy programs (Privacy Manager); and
 - (6) Assist the Commission's B/Os in the implementation of uniform and consistent policies and standards governing the acquisition, maintenance, and use of computers and other electronic or telecommunications equipment in the collection, compilation, maintenance, use, or dissemination of Privacy Act records.
- (D) The **Privacy Manager (PM)** or the PM's designee coordinates and manages the day-to-day duties and responsibilities of the FCC's privacy program with guidance from the SAOP and CIO,⁶⁷ and shall
- (1) Ensure the Commission's implementation of information privacy protections, to ensure ongoing compliance with Federal laws, regulations, and policies relating to information privacy;
 - (2) Manage, coordinate, and facilitate the agency's implementation of all privacy compliance efforts including the annual FISMA submission;
 - (3) Ensure that FCC personnel and contractors receive appropriate training and education programs regarding privacy laws, regulations, policies, and procedures for handling PII;

⁶⁵ 2011 FISMA Report, "privacy section," 8b.

⁶⁶ OMB Memorandum M-05-08, at 2.

⁶⁷ E-mail from the OGC Privacy Legal Advisor, March 9, 2005 citing Section 552(a) of the FY 05 Appropriations Act.

- (4) Implement all FCC Data Integrity Board activities;
 - (5) Supervise the Commission's response(s) to public inquiries about information contained in the FCC's system of records;
 - (6) Administer the systems of records, including the publication of the system of records notices (SORNs) in the *Federal Register*;
 - (7) Conduct Privacy Threshold Analyses (PTA) and the Privacy Impact Assessments (PIA) for the agency's information systems, including both paper-based document files and electronic information systems and databases;
 - (8) Respond to public inquiries, including the Freedom of Information Act (FOIA) requests, about information contained in the FCC's systems of records;
 - (9) Work with the Privacy Legal Advisor in OGC to provide guidance and to respond to B/O questions concerning privacy issues;
 - (10) Compile the Commission's responses for the SAOP (privacy) section of the annual Federal Information Security Management Act (FISMA) report;
 - (11) Assist the SAOP with the Data Integrity Board (DIB), including acting as the DIB secretary and drafting the annual DIB report for distribution to the FCC Chairman, the Head of the Office of Information and Regulatory Affairs at OMB, and the public; and
 - (11) Participate with the SAOP, CIO, and the Privacy Legal Advisors as the Commission's liaisons with the OMB and other Federal agencies.
- (E) The **Privacy Legal Advisors** in the Office of the General Counsel (OGC) shall provide advice, guidance, and interpretation on all legal matters related to the administration of the FCC privacy program.
- (F) **Bureau and Office Chiefs** (or their designees) shall:
- (1) With the guidance from the SAOP, CIO, and PM, ensure that employees and contractors are, at the required intervals, trained in, understand, and follow the requirements of the Privacy Act in the performance of their job duties and responsibilities.
 - (2) With guidance from the SAOP, CIO, and PM ensure that the personnel who require access to PII are mindful of their responsibilities to safeguard PII at their workstation, in the other parts of the FCC's headquarters and/or branch offices, and when telecommuting from home or another approved workplace.
- Note:** All employees who are approved to participate in the telework program, must sign the "Request to Participate in the FCC Flexible Workplace Program" certification. This requirement puts employees on notice that they must:

- (a) Apply the FCC-approved privacy safeguards to protect government data, including PII, from any potential privacy risks such as unauthorized disclosures or damage; and
 - (b) They must comply with the requirements of the Privacy Act when telecommuting.
- (3) Require this same responsibility to safeguard PII to contractors working at FCC headquarters, branch offices, and facilities.⁶⁸

1-7. Criminal Penalties for Privacy Act Violations.

- (A) **Unauthorized Disclosure:** Any officer or employee of the FCC, who by virtue of his/her employment or official position, has possession of, or access to, Commission records which contain PII, the disclosure of which is prohibited by this section, 5 U.S.C. 552a(i), or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any matter to any person or Federal agency not entitled to receive it, shall be guilty of a **misdemeanor** and fined not more than **\$5,000**.⁶⁹

Information in a system of records can only be disclosed with the prior written consent of the individual subject⁷⁰ or for the reasons for nonconsensual disclosure, *i.e.*, unless disclosure of the record would be for one of the routine disclosures listed in 5 U.S.C. 552a(b);⁷¹ in the exceptions to records disclosure listed in 47 CFR § 0.555(b); or in the case of a data breach as provided in OMB Memorandum M-07-16.⁷²

- (B) **Failure to Publish a System Notice:** Any officer or employee of the FCC who willfully maintains a system of records without meeting the notice requirements under 5 U.S.C. § 552a(e)(4) of the *Privacy Act of 1974*, as amended, shall be guilty of a **misdemeanor** and fined not more than **\$5,000**.⁷³

Note: The public notice requirements are set out in Chapter 6.

- (C) **Obtaining Records under False Pretenses:** Any person who knowingly and willfully requests or obtains any record concerning an individual from the FCC or other Federal agency under false pretenses shall be guilty of a **misdemeanor** and fined not more than **\$5,000**.⁷⁴ This applies to anyone inside or outside the Commission.⁷⁵

⁶⁸ 5 U.S.C. 552a(m).

⁶⁹ 5 U.S.C. 552a(i)(1).

⁷⁰ 5 U.S.C. 552a(b); 47 CFR §§ 0.554 and 0.555.

⁷¹ 5 U.S.C. 552a(b); 47 CFR § 0.555(b).

⁷² OMB Memorandum M-07-16, May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," Attachment 2 (B)(2)(b) "Develop and Publish a Routine Use," at 11.

⁷³ 5 U.S.C. 552a(i)(2).

⁷⁴ 5 U.S.C. 552a(i)(3); 47 CFR §§ 0.554(b)(1) and (b)(2), and 0.560.

⁷⁵ 5 U.S.C. 552a(i)(3); 47 CFR § 0.560.

CHAPTER 2

COLLECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

2-1. Policy. The FCC collects, maintains, uses, stores, and disposes of significant amounts of information about individuals (PII) in the course of the Commission's duties and responsibilities under the *Communications Act of 1934*, as amended, and other Federal regulations.¹

(A) Unlike many other types of information, PII must generally be considered sensitive in nature, since the loss or unintentional or unauthorized disclosure of an individual's PII can result in substantial harm, embarrassment, and inconvenience to that individual. Such a loss may lead to identity theft or other fraudulent uses of this information.²

(B) Due to this sensitivity, the Commission requires employees and contractors to exercise sufficient care when they collect, maintain, use, and dispose of PII (when no longer needed), including SSN data, in carrying out their job duties.³

(C) These policy recommendations are part of the Commission's continuing efforts to prevent any inadvertent disclosure or misuse, such as happens when there is a data breach.⁴

Note: The *FCC Breach Notification Policy* (version 6) is found at:
http://intranet.fcc.gov/docs/omd/perm/policies_and_procedures/Breach%20Notification%20Policy%20Sept%202015.pdf

2-2. Reducing Holdings of PII and SSNs. Because of the potential issues and problems associated with the collection and use of PII, it has become increasingly necessary for the Commission to take additional steps to safeguard the PII in the documents, files, and records maintained by the B/Os.⁵

(A) Following guidelines provided by the Office of Management and Budget (OMB) and the Office of Personnel Management, it is the Commission's policy to reduce or eliminate whenever possible, the unnecessary uses of PII,⁶ including Social Security Numbers (SSNs).⁷

Note: The full list of OPM guidelines that the FCC has adopted as part of its commitment to reducing the uses of personally identifiable information (PII) and eliminating Social

¹ OMB Memorandum M-06-15, May 22, 2006, *Safeguarding Personally Identifiable Information*, at 1.

² OMB Memorandum M-06-15, May 22, 2006, *Safeguarding Personally Identifiable Information*, at 1; OMD Memorandum on PII (2007).

³ OMD Memorandum on PII (2007).

⁴ OMB Memo M-07-16, May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, at 1.

⁵ OMB Memo M-07-16, May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, at 1.

⁶ OMB Memorandum M-07-16, at 6.

⁷ OMB Memorandum M-07-16, at 7; OPM Memorandum, *Guidance on Protecting Federal Employee Social Security Numbers and Combatting Identity Theft*, June 18, 2007, at 1.

Security Numbers (SSNs), whenever possible, as required by the Federal Information Security and Management Act (FISMA) is found at:

Appendix 1, *Guidelines for Protecting Social Security Numbers (SSNs) and Other Personally Identifiable Information (PII)*.

- (B) The Managing Director has instructed the SAOP to require all B/Os to review their holdings of all PII and SSN uses on an annual basis. The SAOP has determined that the Commission's review will coincide with the annual FISMA review.⁸
 - (C) This review must ensure, to the maximum extent practicable for each B/O, that:
 - (1) The PII holdings are accurate, relevant, timely, and complete;⁹
 - (2) The PII that is being collected, maintained, used, and stored is the minimum necessary for the proper performance of the Commission's functions;¹⁰ and
 - (3) Access to this PII is restricted to those employees and contractors who must have access as part of their job duties and responsibilities.
 - (D) As part of this annual review, the B/O are also required to examine their uses of SSN information to:
 - (1) Identify instances in which the collection or use of the SSN is superfluous or by which the B/O can devise a method to minimize the use of the full SSN;¹¹ and
 - (2) Establish a plan by which each B/O will eliminate the unnecessary collection and use of SSNs.¹²
 - (E) The results of these two Commission-wide annual reviews of PII and SSN usage will be include as addenda in the SAOP's component of the annual FISMA report that is submitted to OMB and Congress.
 - (F) The Commission participates in government-wide efforts to explore alternatives to Federal agencies' uses of SSNs as personal identifiers for both Federal employees and in Federal programs such as surveys and data calls.¹³
- 2-3. Collecting Social Security Numbers (SSN). The FCC is committed to reducing the use of SSNs whenever possible. However, in those instances where the Commission must ask an individual to provide his/her SSN, it is the Commission's policy that:

⁸ OMB Memorandum M-07-16, at 6. OMB guidelines initially required this PII review to be made public schedule and published in the *Federal Register*.

⁹ OMB Memorandum M-07-16, at 6; OMD Memorandum (2007).

¹⁰ OMB Memorandum M-07-16, at 6 – 7; OMD Memorandum (2007).

¹¹ OMB Memorandum M-07-16, at 7.

¹² OMB Memorandum M-07-16, at 7.

¹³ OMB Memorandum M-07-16, at 7.

- (A) Individuals will not be denied any lawful right, benefit, or privilege if they refuse to provide their social security number (SSN) unless the disclosure of the SSN is required by Federal statute or regulation in effect before January 1, 1975.¹⁴
- (B) When collecting the SSN, the Commission will issue a statement to each individual that lists:¹⁵
 - (1) Whether disclosing the SSN is mandatory or voluntary. A disclosure is voluntary unless a specific legal penalty exists for not providing it.¹⁶
 - (2) The Federal law or Executive Order that established the program or office needing the record.¹⁷
 - (a) The purpose—what use FCC will make of the number.¹⁸
 - (b) What disclosures of the number will be made outside the FCC.¹⁹
 - (c) The effect, if any, of not providing the SSN.²⁰
 - (2) The SSN statement may be combined with the Privacy Act Statement (or Notice), *e.g.*, the Privacy Act Statements required on FCC forms, the FCC websites, and third party websites to which the Commission provides information directly or via a link.²¹

2-4. Privacy Act Statement. When PII (including SSN data) is requested from individuals in connection with FCC programs, including surveys, forms, registration or mailing lists, and other documents and places, a **Privacy Act Statement (or Privacy Notice)** must be provided. The Privacy Act Statement permits the individual, from whom PII is being requested, to make an informed decision on the nature of the request and whether or not to provide the PII.

Privacy Act Statements shall normally appear on the documents, including paper format and electronic documents and forms, and webpages, but they may also be read aloud to individuals, such as when the Commission conducts surveys, when individuals call the FCC Help Line seeking information, or other situations in which the Commission is soliciting PII but a written Privacy Act Statement is not appropriate.²²

The **Privacy Act Statement** (or **Privacy Act Notice**) must include the following:

¹⁴ 5 U.S.C. 552a Note (Section 7(a)(1) of the Act); 47 CFR § 0.554(b)(1) Note.

¹⁵ 5 U.S.C. 552a Note (Section 7(a)(1) of the Act);

¹⁶ 5 U.S.C. 552a Note (Section 7(b) of the Act);

¹⁷ 5 U.S.C. 552a(e)(3)(A).

¹⁸ 5 U.S.C. 552a(e)(3)(B).

¹⁹ 5 U.S.C. 552a(b) and 552a(3)(C).

²⁰ 47 CFR § 0.554(b)(1) Note..

²¹ 5 U.S.C. 552a(e)(3); *1995 FCC Privacy Act Manual*, at 10; OMD Memorandum M-23-10, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010, at 3ff; CIO Council, *Privacy Best Practices for Social Media* (July 2013).

²² 5 U.S.C. 552a(e)(3).

- (A) The legal **authority** (whether granted by Federal statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary.²³
- (B) The **principal purpose(s)** for which the information is intended to be used.²⁴
- (C) The **routine use(s)** which may be made of the information, as published pursuant to 5 U.S.C § 552a(e)(4)(D) of the Privacy Act. These are the disclosures, if any, which will be made outside of the FCC.²⁵
- (D) Whether the **disclosure** is voluntary or mandatory. Furnishing the information is mandatory only if there is a specific penalty under law, Executive Order, or regulation for not doing so.²⁶

The **effects** on the individual, if any, of not providing all or any part of the requested information.²⁷ For instance, it may be impossible to issue a license without the requested information.²⁸

²³ 5 U.S.C. 552a(e)(3)(A).

²⁴ 5 U.S.C. 552a(e)(3)(B).

²⁵ 5 U.S.C. 552a(e)(3)(C).

²⁶ 5 U.S.C. 552a(e)(3)(A); *1995 FCC Privacy Act Manual*, at.9

²⁷ 5 U.S.C. 552a(e)(3)(D).

²⁸ 5 U.S.C. 552a(e)(3)(D); *1995 FCC Privacy Act Manual*, at 10.

CHAPTER 3

DISCLOSING PERSONALLY IDENTIFIABLE INFORMATION (PII) IN RECORDS

- 3-1. **Policy.** It is the FCC's policy to safeguard all PII in the Commission's possession, and to disclose this PII, only as appropriate, subject to certain limitations, as provided by the Commission's rules¹ and the exemptions specified in the Privacy Act, 5 U.S.C. 552a(j) – a(k).² This policy is designed to ensure that only an individual who is entitled to his/her information may obtain it and to avoid any unauthorized disclosure of information, *e.g.*, privacy breach.³
- 3-2. **Disclosures from Systems of Records.** A **disclosure** is the transfer of information by any means from a system of records to anyone other than the subject of the record or the authorized agent acting for the subject.⁴
- (A) The Privacy Act does not require the Commission to disclose any record, *i.e.*, PII, to anyone other than the subject,⁵ except when ordered to do so by a court,⁶ or when the record is requested under the Freedom of Information Act (FOIA) and cannot be withheld under a FOIA exemption.⁷ In no case can the Act be used to deny information that is required to be disclosed under FOIA.⁸
- (B) FCC employees who are responsible for maintaining, collecting, using, and disseminating personal information should become equally familiar with FCCINST 1179.1, *Freedom of Information Act* (FOIA), under 5 U.S.C. 552.⁹ The FCC Internet FOIA webpage is found at: <https://www.fcc.gov/general/foia>.
- 3-3. **Disclosures.** There are three types of information **disclosures**—the transfer of information by any means from a system of records to anyone other than the subject of the record or the authorized agent acting for the subject.¹⁰ These are consensual disclosures, unauthorized disclosures, and disclosures that do not requiring the consent of the individual (or subject or the information).
- (A) **Consensual Disclosures.** The FCC should not disclose any record (*i.e.*, PII) which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be for one of the reasons set forth in Section 3-4 below.¹¹

¹ 47 CFR §§ 0.555(b)(1) – (b)(2).

² 5 U.S.C. 552a(j) – a(k);

³ 47 CFR §§ 0.554 - 0.555; 5 U.S.C. 552a(j) – (a)(k).

⁴ 5 U.S.C. 552a(b); 47 CFR §§ 0.554(a) and 0.555(a)-(b).

⁵ 5 U.S.C. 552a(b) and 552a(t); 47 CFR §§ 0.554 - 0.555.

⁶ 5 U.S.C. 552a(b)(11).

⁷ 5 U.S.C. 552, 552a(b)(2), and 552a(t).

⁸ 5 U.S.C. 552, 552a(b)(2), and 552a(t).

⁹ 5 U.S.C. 552; 47 CFR §§ 0.441 – 0.470.

¹⁰ 5 U.S.C. 552a(b); 47 CFR §§ 0.554 - 0.555.

¹¹ 5 U.S.C. 552a(b).

- (B) **Unauthorized Disclosure.** Knowingly and willfully disclosing information from a system of records to any party not entitled to receive it by any officer or employee of the FCC may be subject to criminal penalties, *e.g.*, a data breach.¹²

Note: The FCC Breach Notification Policy is found at:

http://intranet.fcc.gov/docs/omd/perm/policies_and_procedures/Breach%20Notification%20Policy%20Sept%202015.pdf

- (C) **Disclosures not requiring the Subject's Consent.** The Privacy Act lists various types of disclosures or **routine uses** for which prior consent of the individual is not required if the disclosure is:

- (1) To those officers and employees of the FCC who have a need for the record in the performance of their duties.¹³
- (2) Required under the FOIA, 5 U.S.C. 552.¹⁴ If a FOIA request involves personal information (*i.e.*, PII), and FOIA does not require its disclosure,¹⁵ *i.e.*, covered by one of the FOIA exemptions, the consent of the individual must be obtained prior to disclosure unless the disclosure is permitted under one of the conditions listed in this section, 5 U.S.C. 552a(b) of the Act.¹⁶
- (3) For a routine use as defined under 5 U.S.C. 552a(a)(7) of the Act and described under 5 U.S.C. 552a(e)(4)(D) and which has been published in a notice in the *Federal Register*.¹⁷
- (4) To the Bureau of the Census for the purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13.¹⁸
- (5) To a recipient who has provided the Commission with prior, adequate, written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.¹⁹
- (6) To the National Archives and Records Administration (NARA) as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value.²⁰

¹² 5 U.S.C. 552a(t)(1).

¹³ 5 U.S.C. 552a(b)(1).

¹⁴ 5 U.S.C. 552a(b)(2).

¹⁵ 5 U.S.C. 552; FOIA under 5 U.S.C. 552(b) or www.fcc.gov/foia; 47 CFR §§ 0.441- 0.470.

¹⁶ 5 U.S.C. 552a(b) and 552a(t).

¹⁷ 5 U.S.C. 552a(b)(3).

¹⁸ 5 U.S.C. 552a(b)(4).

¹⁹ 5 U.S.C. 552a(b)(5).

²⁰ 5 U.S.C. 552a(b)(6) and 552a(l).

Note: Records transferred to a Federal Records Center and private records storage facilities for safekeeping and storage do not fall within this category. These remain under the legal custody of the FCC.²¹

- (7) To another Federal agency or to an instrumentality of any Federal, state, or local governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency, which maintains the record, specifying the particular portion desired and the law enforcement activity for which the record is sought.²²
- (8) To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.²³

The affected individual need not be the subject of the record disclosed. Examples of compelling circumstances are medical emergencies, accidents, or epidemics. When such a disclosure is made, notify the individual subject at his or her last known address.²⁴

- (9) To either House of Congress, or, to the extent of the matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee.²⁵
- (10) To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office.²⁶
- (11) Pursuant to the order of a court of competent jurisdiction.²⁷
- (12) To a consumer reporting agency (credit bureaus) in accordance with the *Federal Claims Collection Act of 1966*, under 31 U.S.C. 3711(e).²⁸

- 3-4. Restrictions on Routine Use Disclosures. PII in a system of records may be disclosed under one or more of the 12 routine uses listed in the Privacy Act and/or other, additional routine uses that the Commission has employed that pertain to specific uses and/or circumstances for its SORNs; however, the Commission has also included a caveat for any (routine use) disclosure(s):

In each case the FCC will determine whether disclosure of the records is compatible with the purpose(s) for which the records are collected.

- 3-5. Standards and Balances Affecting Disclosure.

²¹ 5 U.S.C. 552a(l)(1).

²² 5 U.S.C. 552a(b)(7).

²³ 5 U.S.C. 552a(b)(8); 47 CFR § 0.555(b)(1).

²⁴ 5 U.S.C. 552a(b)(8); 47 CFR § 0.555(b)(1).

²⁵ 5 U.S.C. 552a(b)(9).

²⁶ 5 U.S.C. 552a(b)(10).

²⁷ 5 U.S.C. 552a(b)(11).

²⁸ 5 U.S.C. 552a(b)(12).

- (A) For all disclosures outside of the FCC, except for releases made under FOIA, system managers shall ensure that the records are accurate, timely, complete, and relevant for Commission purposes.²⁹
- (B) All records must be disclosed if their release is required by the FOIA,³⁰ unless they are exempted from disclosure by one of the nine FOIA exemptions.³¹ For example, FOIA Exemption No. 6 denies the release of most personnel, medical, or similar records when it would be a “clearly unwarranted invasion of personal privacy.”³²

Note: The FCC's FOIA webpage at www.fcc.gov/foia provides a complete discussion of the Commission's FOIA policies and regulations, including the nine exemptions.

- 3-6. Federal Employee Information. Disclosures of information regarding Federal employees shall be made in accordance with the Federal Personnel Manual.³³

Note: Chapter 8 also contains information regarding Federal requirements concerning the FCC's Human Resources Management division's maintenance of personnel folders and other documents on FCC employees.

Some examples of information regarding FCC employees that normally may be released without unwarranted invasion of personal privacy include:

Name
Present and past position titles
Present and past grades
Present and past salaries
Present and past duty stations
Current office telephone number

- 3-7. Discretion in Disclosure. Discretion is advised when making disclosures to third parties.³⁴ The B/Os considering making nonconsensual disclosures, other than those disclosures “not requiring the subject's consent,” should consult the OGC Privacy Legal Advisors for advice. A balancing test is advised for such disclosures. Thus, a disclosure, which normally would require the individual's consent, may be made if:

- (A) The disclosure would benefit the individual,³⁵

²⁹ 5 U.S.C. 552a(e)(6).

³⁰ 5 U.S.C. 552a(b)(2) and 552a(t).

³¹ 5 U.S.C. 552(b).

³² 5 U.S.C. 552(b)(6).

³³ Contact HRM for access to and assistance with the Federal Personnel Manual.

³⁴ 5 U.S.C. 552a(b); 47 CFR § 0.554(b).

³⁵ 5 U.S.C. 552a(b)(8).

- (B) The disclosure would be in the public interest, *i.e.*, as under FOIA and the public's need to understand the operations of the government outweighs the individual's right to privacy.³⁶

³⁶ 5 U.S.C. 552a(b)(2) and 552a(t).

CHAPTER 4

ACCESS, AMENDMENT, AND APPEALS BY INDIVIDUALS

- 4-1. **Policy.** As provided in the *Privacy Act of 1974*, as amended, 5 U.S.C. 552a(f), individuals may exercise their rights to ask if the FCC maintains any records (*i.e.*, PII) on them in any system(s) of records.¹ If such records exist, individuals have the rights of access to the records;² to request amendment of the records (if applicable);³ and to appeal of the FCC's decisions to deny them access or amendment of the records.⁴
- 4-2. **Access Requests, Appeals, and Amendments.** The FCC has specific, detailed procedures for processing the various types of requests and appeals possible under the Privacy Act. The terms related to these procedures include:
- (A) **Access Request.** An individual's request to see or receive a copy of records about him/her in a system of records.⁵ First, the Commission must determine if the individual is a subject of a record in the specified system of records, and notify the requester whether a record exists.⁶
 - (B) **Appeal of Denied Access.** An individual's request for administrative review of the Privacy Officer's decision to deny access to a Privacy Act record.⁷
 - (C) **Amendment Request.** An individual's request to amend or correct records found to be in error (not accurate, timely, complete, or relevant).⁸
 - (D) **Appeal of Denied Amendment.** This can include: (1) administrative appeal of the decision to deny amendment;⁹ and (2) challenging refusal to amend by having a statement of disagreement posted with the record.¹⁰
 - (E) **Court Action.** This results from individual's suit for judicial review of agency refusal to amend or grant access to a record of which he/she is the subject.¹¹

¹ 5 U.S.C. 552a(f)(1); 47 CFR § 0.554(a).

² 5 U.S.C. 552a(b)(2), 552a(d)(1), and 552a(f)(2) and (f)(3); 47 CFR § 0.555; OMB Circular A-130, at 8(a)(1)(k)(5)(b).

³ 5 U.S.C. 552a(d)(2) and 552a(f)(4); 47 CFR § 0.556; OMB Circular A-130, at 8(a)(1)(k)(9)(d).

⁴ 5 U.S.C. 552a(d)(3) and 552a(f)(4); 47 CFR §§ 0.555(e), 0.556, and 0.557.

⁵ 5 U.S.C. 552a(d)(1) and 552a(f)(1); 47 CFR §§ 0.554(a) and 0.555; OMB Circular A-130, at 8(a)(1)(k)(9)(d).

⁶ 5 U.S.C. 552a(f)(1); 47 CFR § 0.554(a).

⁷ 5 U.S.C. 552a(d)(2)(B)(ii) and 552a(d)(3); 47 CFR § 0.556(e).

⁸ 5 U.S.C. 552a(d)(2)(B)(i), 552a(e)(6), and 552a(f)(4); 47 CFR § 0.556(a); OMB Circular A-130, at 8(a)(1)(k)(9)(d).

⁹ 5 U.S.C. 552a(d)(3) and 552a(f)(4); 47 CFR §§ 0.555(e)(1), 0.556(c)(2)(ii) and (c)(2)(iii), and 0.557.

¹⁰ 5 U.S.C. 552a(d)(3) and 552a(f)(4); 47 CFR §§ 0.557(d)(2) and (d)(3).

¹¹ 5 U.S.C. 552a(d)(3) and 552a(g)(1) and (g)(2)(A); 47 CFR §§ 0.555(e)(2) and 0.557(d)(4).

4-3. Conditions for Requests.

- (A) To be considered a “Privacy Act request,” a request must come from the individual who is the subject of a record in a system of records,¹² or from his/her designated agent or legal guardian.¹³ The subject must be a **U.S. citizen** or **permanent resident alien**.¹⁴
- (B) The requester must reasonably describe the records sought:
 - (1) The Commission does not accept blanket requests for “all records about me,” or similarly “vague” requests.¹⁵
 - (2) Requests must be for specific information or documents contained in one or more of the systems of records maintained by the FCC, which are posted on the FCC Privacy webpage at:
<https://www.fcc.gov/general/privacy-act-information#systems>.
 - (3) The Privacy Manager will send the requester the Commission’s initial letter or e-mail (if an e-mail address is provided) acknowledging receipt of the request.
 - (4) If the requester has not specified which systems of record to be searched, the Privacy Manager will ask the requester to provide such a list.¹⁶
 - (5) Upon receipt of the requester’s list of systems of records (in response to the Commission’s initial response letter), the Privacy Manager will then forward this request to the appropriate system manager in the bureau/office (B/O) where that system(s) of records is located.¹⁷
 - (6) If any records are found, the system manager in the B/O must make the determination about whether to release the record(s) to the requester, in consultation with the OGC Privacy Legal Advisor(s), SAOP, and other B/O and privacy officials.¹⁸
 - (7) Their decision will be guided by the Commission’s procedures and regulations under 47 CFR §§ 0.554ff of FCC Rules and 5 U.S.C. 552a of the Privacy Act, as explained in this Chapter.
- (C) All request for records or information about a requester sent by regular mail must be signed by the individual requester and must include his/her printed name, current address, telephone number (if available), and e-mail address (if available).¹⁹

¹² 5 U.S.C. 552a(f)(1) and 552a(f)(2); 47 CFR §§ 0.554(a) and 0.555(a).

¹³ 5 U.S.C. 552a(h)

¹⁴ 5 U.S.C. 552a(a)(2); 47 CFR § 0.551(b)(1).

¹⁵ 47 CFR § 0.554(a).

¹⁶ 47 CFR § 0.554(a).

¹⁷ 47 CFR § 0.554(a).

¹⁸ 47 CFR §§ 0.554(c) and 0.555.

¹⁹ 47 CFR §§ 0.554(b)(2).

Note: Section 4-10 explains the Commission’s requirements to verify the identity of the requester.

4-4. Systems of Records.

(A) The Commission publishes in the *Federal Register* upon establishment or revision a notice of the existence and character (description) of each system of records notice (SORN), which includes **16 data elements (or headings or sections)**.²⁰ These 16 data elements are explained fully in Chapter 6.

(B) The FCC’s Internet Privacy Act webpage at: <https://www.fcc.gov/general/privacy-act-information#systems> lists the systems of records that are currently maintained by the Commission:

(1) A table of contents, which is alphabetized by B/O, precedes the description of each system of records.²¹ The systems of records provide a “hot link” to the system’s description that was published in the *Federal Register* Notice.

(2) This “arrangement” allows the inquirer to identify easily any or all systems of records of interest to him/her, as described in the *Federal Register* Notice.²²

Note: In circumstances where a requestor cannot access the FCC’s Privacy Act webpage, the Privacy Manager may include a copy of this information in the Commission’s response letter or e-mail.

(C) The FCC’s Internet Privacy Act webpage at: <https://www.fcc.gov/general/privacy-act-information#systems> also lists the citation for all publication dates of the SORNs in the *Federal Register*.²³

(1) This is in accordance with 5 U.S.C. 552a(e)(3) – (e)(4) of the Privacy Act and OMB regulations.²⁴

(2) These regulations require the FCC to publish a notice in the *Federal Register* to inform the public whenever the Commission proposes:²⁵

(a) To establish new system(s) of records;²⁶

²⁰ National Archives and Records Administration (NARA), *Document Drafting Handbook*, at 3-23.

²¹ 47 CFR § 0.554(a).

²² 47 CFR § 0.554(a).

²³ 47 CFR § 0.554(a).

²⁴ 5 U.S.C. 552a(e)(3), (e)(4), and (e)(11); 47 CFR § 0.552; OMB Circular A-130, (Nov. 2000), Appendix I., 4(c), 4(e), 5, and 5(a).

²⁵ 5 U.S.C. 552a(e)(3), (e)(4), and (e)(11); 47 CFR § 0.552; OMB Circular A-130, (Nov. 2000), Appendix I., 4(c), 4(e), 5, and 5(a).

²⁶ 5 U.S.C. 552a(e)(3), (e)(4), and (e)(11); 47 CFR § 0.552; OMB Circular A-130, (Nov. 2000), , Appendix I., 4(c) 4(e), 5, and 5(a).

- (b) To make substantive changes to any existing system(s) of records;²⁷ and/or
- (c) To cancel any system(s) of records (*e.g.*, if they are no longer needed or are obsolete).²⁸

4-5. Requests under the *Freedom of Information Act* (FOIA) versus the Privacy Act.

- (A) An individual should cite or make reference to the Privacy Act in making his/her request, and should note on the envelope, in their e-mail, or FOIA request that it is a “Privacy Act Request;” otherwise the letter will be handled as ordinary mail.²⁹
- (B) Likewise, a request that only cites “FOIA” is not generally treated as a Privacy Act request unless the individual asks for “all information about me” or similar language in the request.³⁰ Please note that an individual who requests both Privacy Act and FOIA information must indicate these dual purposes in making the request.

Note: The Commission has, however, generally treated requests for “all information/records about me” as Privacy Act requests.

- (C) The Privacy Act and FOIA serve different purposes.³¹ Employees who are involved with processing public requests should become familiar with procedures under both Acts. They should observe the following guidance:
 - (1) Follow **FCCINST 1179.2**, *Freedom of Information Act* when handling FOIA requests.
 - (2) The FCC’s Internet FOIA webpage at: <https://www.fcc.gov/general/foia-0> provides a complete discussion of the Commission’s FOIA policies and regulations, including the nine exemptions.
 - (3) The Privacy Act intersects with Exemption 6 of FOIA, which protects any “personal, medical, and similar information, the disclosure of which would constitute a clearly unwarranted invasion of privacy.”

Note: FCC staff are advised to exercise caution in releasing any PII—nothing in the Privacy Act provisions requires disclosure.³² For guidance refer to the FCC FOIA webpage and/or consult OGC’s Privacy Legal Advisors.

²⁷ 5 U.S.C. 552a(e)(3), (e)(4), and (e)(11); 47 CFR § 0.552; OMB Circular A-130, (Nov. 2000), Appendix I, 4(c) 4(e), 5, and 5(a).

²⁸ 5 U.S.C. 552a(e)(3), (e)(4), and (e)(11); 47 CFR § 0.552; OMB Circular A-130, (Nov. 2000), Appendix I, 4(c) 4(e), 5, and 5(a).

²⁹ 47 CFR § 0.554(a).

³⁰ 5 U.S.C. 552a(t).

³¹ 5 U.S.C. 552a(b)(2) and 552a(t).

³² 47 CFR §§0.554(b), 0.555(b), 0.555(d), and 0.561; 5 U.S.C. 552a(b), 552a(e)(6), 552a(e)(10), 552a(f)(3), 552a(j), 552a(k), and 552a(t).

- (4) If an individual cites both the Privacy Act and the FOIA, the FOIA Office will process the request under both Acts in the manner that gives the most information and is yet consistent with the form and content of the Privacy Act law provisions.³³
- (5) An individual who requests access to his/her records should be allowed access to them, as required under 5 U.S.C. 552a(d) and (f), except under those circumstances specified in FCC Rules under 47 CFR §§ 0.555(b), (d), and (e), which provide guidance in determining whether the Commission may seek to deny access to all or part of a record.³⁴ See Section 4-12ff.
- (6) When a requester seeks information about someone who is **deceased**, this is generally treated as a FOIA rather than a Privacy Act request, as deceased individuals do not have any Privacy Act right, nor do executors or next-of-kin.³⁵ However, the requester must provide evidence that the individual is deceased such as an obituary or death notice. The OGC Privacy Legal Advisors should be consulted for guidance in this case.

4-6. Inquiries and Questions. The Privacy Manager and the OGC Legal Advisors provide guidance and assistance when:³⁶

- (A) Individuals have questions regarding the Commission's Privacy Act procedures for:
 - (1) Gaining access to a particular system of records, and/or who request clarification of a *Federal Register* Notice;
 - (2) The description of specific systems of records set forth in the *Federal Register* Notice; or
 - (3) Requesting amendment of a record.³⁷

³³ 5 U.S.C. 552 at www.fcc.gov/foia, and 552a(b)(2), 552a(d), 552a(f), and 552a(t).

³⁴ 47 CFR §§ 0.555(b), (d), and (e).

³⁵ See OMB Guidelines, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf; see also *Warren v. Colvin*, 744 F.3d 841, 843-44 (2d Cir. 2014) (“[plaintiff] correctly asserts that deceased individuals generally do not enjoy rights under the Privacy Act”); *Whitaker v. CIA*, 31 F. Supp. 3d 23, 48 (D.D.C. 2014) (“The Privacy Act does not speak to the access rights of relatives of deceased individuals”; deferring to agency’s interpretation based on OMB’s guidance that precludes “the exercise of Privacy Act rights by relatives on behalf of deceased individuals”).

³⁶ 47 CFR §§ 0.556(a); 5 U.S.C. 552a(d)(2) and 552a(t)(4).

³⁷ 47 CFR §§ 0.556(a); 5 U.S.C. 552a(d)(2) and 552a(t)(4).

The Privacy Manager may be contacted³⁸ by telephone: (202) 418-0217; by e-mail: Privacy@fcc.gov; or by writing to:

Privacy Manager
Information Technology
Federal Communications Commission (FCC)
445 12th Street, SW
Washington, D.C. 20554

- (B) Individuals make requests to **amend** a record and/or to **contest** the contents of a record, either administratively or judicially, should contact the Privacy Legal Advisor in the Office of General Counsel (OGC)³⁹ by addressing these inquiries to:

Privacy Legal Advisor
Office of the General Counsel (OGC)
Federal Communications Commission (FCC)
445 12th Street, SW
Washington, D.C. 20554

- (C) Individuals make requests relating to **official personnel records** of current FCC employees,⁴⁰ including requests to amend records,⁴¹ should be submitted to:

Chief Human Capital Officer
Human Resources Management
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

- (D) Individuals make requests related to official personnel records of former FCC employees, including requests to amend records, should be sent to:⁴²

Assistant Director for Work Force Information
Compliance and Investigations Group
Office of Personnel Management (OPM)
1900 E Street, NW
Washington, DC 20415

4-7. Making a Privacy Act Request.

- (A) Under FCC Rules, 47 CFR § 0.554, an individual may make a Privacy request, in one of several ways—you may:⁴³

³⁸ 47 CFR §0.558.

³⁹ 47 CFR § 0.558.

⁴⁰ 47 CFR §§ 0.554(c); 5 U.S.C. 552a(f)(3) and (f)(4).

⁴¹ 47 CFR §§ 0.556(a); 5 U.S.C. 552a(d)(2), 552a(f)(3), and (f)(4).

⁴² 47 CFR § 0.555(a) is regulation citing where to send requests for amendment of records, but OPM is also the location for information on files of former FCC employees; 5 U.S.C. 552a(d)(2), 552a(f)(3), and (f)(4).

⁴³ 47 CFR §§ 0.554(c) and 0.555(a); 5 U.S.C. 552a(d)(1), 552a(f)(1), (f)(2), and (f)(3).

- (1) Use the electronic Privacy Act (E-Privacy Act) Request Form at:
<https://www.fcc.gov/general/foia>; ⁴⁴
- (2) Send us a privacy request by regular mail (marked “Privacy Request”);⁴⁵
- (3) Fax the FOIA Office in PERM with your privacy request; or
- (4) Visit the FCC Reference Information Center (RIC) to make a privacy request in person (“walk-in”);⁴⁶
 - (a) Due to increased security following September 11, 2001, all visitors to the FCC’s headquarters must be escorted by Commission personnel:
 - (i) A requester should call the Privacy Manager at least **two business days** prior to the proposed visit to schedule an appointment so we can arrange for a Commission employee to escort you to the RIC. ⁴⁷
 - (ii) The requester should also provide a telephone number where you can be reached during the day in case the appointment must be changed.⁴⁸
 - (b) Inspection is only allowed in the RIC between 10:00 a.m. – 3:00 p.m., Monday through Thursday, and between 8:00 a.m. – 11:00 a.m. on Friday.⁴⁹
- (5) The Commission will no longer transfer records to a field office for inspection.⁵⁰
- (B) The requester must name **each** system of records that he/she wishes searched to satisfy the request for information.⁵¹ The list of systems of records maintained by the Commission can be found on the FCC’s Privacy Act webpage at:
<https://www.fcc.gov/general/privacy-act-information#systems>.

As explained above, if the requester (other than a walk-in) does not name the system(s) that he/she wishes searched, the Privacy Manager will send the request a letter or e-mail asking for this information.

4-8. Receipt and Control.

- (A) The Commission has established a centralized administrative system to process Privacy Act requests, with **two exceptions**:

⁴⁴ FCC Privacy Act Webpage.

⁴⁵ 47 CFR § 0.554(a); 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(3).

⁴⁶ 47 CFR §§ 0.555(a)(1) and 0.555(a)(2); 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(3).

⁴⁷ 47 CFR § 0.555(a)(1); 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(3)..

⁴⁸ 47 CFR § 0.555(a)(1); 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(3).

⁴⁹ 47 CFR § 0.555(a)(1).

⁵⁰ 47 CFR § 0.555(a)(2).

⁵¹ 47 CFR § 0.555(a).

- (1) Requests for official personnel records of **current FCC employees** are the responsibility of Human Resources Management (HRM) and should be sent to HRM.⁵² See Section 4-5; and
 - (2) Requests for official personnel records of **former FCC employees** are the responsibility of the Office of Personnel Management (OPM) and should be sent to OPM for action.⁵³ See Section 4-5.
- (B) All letters and e-mail, including those sent via the FCC FOIA e-mail form at: <https://www.fcc.gov/general/foia>, and those sent by regular e-mail, which are identifiable as **PRIVACY REQUESTS** are delivered to the FOIA Office for processing.⁵⁴
- (C) For Privacy requests that it receives, the FOIA Office in PERM will:
- (1) Date stamp each request when it is received,
 - (2) Assign a FOIA (Privacy) Control Number, and
 - (3) Log-in the request to establish the Commission's date of receipt.⁵⁵
 - (4) Send the privacy request to the Privacy Manager for processing.
- (D) Within **10 business days** following receipt of the request, the Privacy Manager will send the requester a letter or e-mail acknowledging the Commission's receipt of the Privacy Act request.
- (E) If the requester has not specified which systems of record to be searched, the Privacy Manager will ask the requester to provide such a list.⁵⁶
- (1) The Commission does not accept blanket requests for "all information about me" nor will the Commission honor a request that lists all the systems of records.⁵⁷
 - (2) The list of systems of records maintained by the Commission may be found by:
 - (a) Accessing the FCC's "Privacy Policy" webpage at: <http://www.fcc.gov/fccprivacypolicy.html>

⁵² 47 CFR § 0.554(c); 47 CFR § 0.556(a) is regulation citing where to send requests for amendment of records, but HRM is also the system manager for current FCC employees.

⁵³ 47 CFR § 0.555(a) is regulation citing where to send requests for amendment of records, but OPM is also the location for information on files of former FCC employees.

⁵⁴ 47 CFR § 0.554(c); 5 U.S.C. 552a(f)(3).

⁵⁵ 47 CFR §§ 0.554(c) and 0.554(d); 5 U.S.C. 552a(f)(1) – (f)(3).

⁵⁶ 47 CFR §§ 0.554(d)(1); 5 U.S.C. 552a(d)(2)(A) and 552a(f)(1)-(f)(3).

⁵⁷ 47 CFR § 0.554(a)

- (b) Go to the “Sharing and Disclosing” subheading and the link to the System of Records located on the [Privacy Act webpage](#) hotlink to the various Privacy Act links:
- (c) Select the Systems of Records webpage: <https://www.fcc.gov/general/privacy-act-information#systems> where the list of the Systems of Records are found and selecting the ones that the requester wishes to be searched.
- (4) The Commission’s acknowledgement letter may, if necessary, request additional information needed to locate any records or to get other information from the requester, *e.g.*, correct address, etc., which is necessary to process the request.⁵⁸

4-9. Responding to a Search Request.

- (A) Upon receipt of the list of system(s) of records that the requester has identified for the Commission to search, the Privacy Manager will send the request to the **System Manager(s)** in the B/O that maintains the system(s) of records in question.⁵⁹
 - (1) A copy of each request is also sent to the Privacy Legal Advisor in OGC.
 - (2) This begins the **30 business day** response period to acknowledge requests and to document the handling, coordination, and completion of each Privacy Act request.⁶⁰
- (B) The **System Manager** in each B/O has responsibility for the system(s) of records named in the privacy request:
 - (1) The system manager will conduct a search of each system of records under his/her responsibility that has been identified in the individual’s request to determine if any records pertaining to the individual are contained therein.⁶¹
 - (2) Once the system manager has obtained the requested records and completed the search, he/she should notify the Privacy Manager as to where the records are located, if they are easily accessible, and whether or not the FCC maintains information about the individual.⁶²
- (C) The system manager must also determine whether or not the requested materials are contained in a system of records that:
 - (1) Is **exempt** or **partially exempt** from disclosure under 47 CFR § 0.561;⁶³

⁵⁸ 47 CFR §§ 0.554(d).

⁵⁹ 47 CFR § 0.554(c); 5 U.S.C. 552a(e)(4)(H) and 552a(f)(1).

⁶⁰ 47 CFR §§ 0.554(d) and 0.555; 5 U.S.C. 552a(c), 552a(d)(2)(A) and 552a(f)(1)-(f)(3).

⁶¹ 47 CFR §§ 0.554(c) and 0.554(d); 5 U.S.C. 552a(f)(1) – (f)(3).

⁶² 47 CFR § 0.554(d); 5 U.S.C. 552a(f)(3).

⁶³ 47 CFR §§ 0.555(b), 0.555(d), and 0.561; 5 U.S.C. 552a(f)(3).

- (2) Is subject to the provisions of 47 CFR §§ 0.555(b) and 0.555(d), which **restrict disclosure** of some types of personal information;⁶⁴ and/or
- (3) Contains materials compiled in anticipation of a **civil action** or **proceeding**.⁶⁵
- (D) If the system manager has questions about disclosing the information, he/she should discuss these concerns with the SAOP, Privacy Legal Advisors, and the FCC's other privacy officials.⁶⁶
- (E) If there are no issues that may restrict disclosure, *e.g.*, difficulty verifying the requester's identity,⁶⁷ or requesting records from a system of records that is **totally** or **partially exempt** from disclosure under 47 CFR §§ 0.555(b) or 0.561 of FCC Rules,⁶⁸ then the system manager will notify the Privacy Manager as soon as the determination is made.⁶⁹
- (F) The system manager should bring the Privacy Manager a copy of the requested materials. The FOIA Office keeps all documents related to this request subject to the National Archives and Records Administration (NARA) approved records retention schedules. The General Records Schedule (GRS) for FOIA documents is seven years.⁷⁰
- (G) The Privacy Manager will send a second letter or e-mail to inform the individual of the results of the search.
 - (1) If the search request found no records pertaining to the individual's request, the Privacy Manager will send the FOIA Office a copy of this second letter and any other documents and all other materials related to this request, and the FOIA Office will close the privacy request.
 - (2) If the search request produced records pertaining to the request, the letter will acknowledge the search results, including information on any charges and payment instructions, when applicable.⁷¹ We will ask the individual:
 - (a) Whether he/she wishes to make an appointment to come to the RIC to inspect the records in person,⁷² or
 - (b) If he/she wishes the Privacy Manager to mail or e-mail a copy of the requested record(s) to him/her, after we have verified the requester's identity.⁷³

⁶⁴ 47 CFR §§ 0.555(b), 0.555(d), and 0.561; 5 U.S.C. 552a(f)(3).

⁶⁵ 47 CFR §§ 0.555(b), 0.555(d), and 0.561; 5 U.S.C. 552a(j) and 0.555a(k).

⁶⁶ OMB Memorandum, M-05-08, *Designation of Senior Agency Officials for Privacy*, February 11, 2005, at 1-2.

⁶⁷ 47 CFR § 0.555(b)(3); 5 U.S.C. 552a(2).

⁶⁸ 47 CFR §§ 0.555(b), 0.555(d), and 0.561; 5 U.S.C. 552a(f)(3), 552a(j), and 0.555a(k).

⁶⁹ 47 CFR § 0.554(d); 5 U.S.C. 552a(f)(1) – 552a(f)(3).

⁷⁰ 5 U.S.C. 552a(c)(1).

⁷¹ 47 CFR § 0.555(c); 5 U.S.C. 552a(f)(5).

⁷² 47 CFR § 0.555(a)(3); 5 U.S.C. 552a(d)(1).

⁷³ 47 CFR §§ 0.554(d) and 0.555(a)(3); 5 U.S.C. 552a(d)(1), 55a(f)(1) – (f)(3)..

Note: The Commission has discontinued the practice of transferring materials to a Commission field office or installation near the requester's home.⁷⁴

- (c) Unless the requester has already provided acceptable ID documents to the FCC, the second letter will also include a request that two documents (from the list of acceptable documents) be furnished to confirm the requester's identity, before the Commission can release the records to the individual requester.⁷⁵

Note: The Privacy Manager may also call or (preferably) e-mail or mail the requester when records are found asking that these ID documents be sent ASAP so that the second letter can include the records (obviating the need to send a third letter).

- (H) Normally, a request should be processed and the individual requester notified of the search results within **30 business days** from the date the inquiry is received (*i.e.*, logged into the system), as required by 47 CFR § 0.554(d) of the FCC Rules.⁷⁶
 - (1) However, if there are extenuating circumstances, *e.g.*, when records have to be recalled from the Federal Records Center, etc., notification may be delayed.⁷⁷
 - (2) Should the System Manager need additional time, he/she should notify the Privacy Manager as to the reasons for the delay.⁷⁸
- (I) The Privacy Manager will call, e-mail, or write the requester to give a projected date for completing the Commission's response:⁷⁹
 - (1) In the FCC's notification for the delay, the Privacy Manager will inform the requester of the reason(s) for the delay and give an approximate date when the record(s) should be available for disclosure.⁸⁰
 - (2) If necessary, the FCC may request additional information needed for the Privacy Manager to coordinate the location and retrieval of the record(s) by the System Manager(s).⁸¹ This is often the situation when requesters list several systems of records in their requests or when the information that they have provided is vague or inaccurate. .
- (J) As noted above, in circumstances where there are no records that are found that pertain to the requester, the Privacy Manager will still send the requester a letter or e-mail

⁷⁴ 47 CFR §§ 0.555(a)(2).

⁷⁵ 47 CFR §§ 0.554(b)(2) and 0.555(a)(3); 5 U.S.C. 552a(f)(2).

⁷⁶ 47 CFR §§ 0.554(d) and 0.555(a)(3); 5 U.S.C. 552a(d)(1), and 552a(f)(1) – (f)(2).

⁷⁷ 47 CFR §§ 0.554(d); 5 U.S.C. 552a(d)(2)(A) and 552a(f)(1) – (f)(2).

⁷⁸ 47 CFR §§ 0.554(d); 5 U.S.C. 552a(d)(2)(A) and 552a(f)(1) – (f)(2).

⁷⁹ 47 CFR §§ 0.554(d); 5 U.S.C. 552a(d)(2)(A) and 552a(f)(1) – (f)(2).

⁸⁰ 47 CFR §§ 0.554(d); 5 U.S.C. 552a(d)(2)(A) and 552a(f)(1) – (f)(2).

⁸¹ 47 CFR §§ 0.554(d); 5 U.S.C. 552a(f)(1) – (f)(3).

informing him/her of this, so that the FCC has a record of this, and the FOIA Office can close this request..

- (K) All documents pertaining to a privacy request, including correspondence, findings (*i.e.*, records pertaining to the request), ID documents, and any other relevant information, must be sent to the FOIA Office as part of their records management responsibilities.⁸²
- (L) If the system manager determines that there are reasons to deny access, in whole or in part, he/she must contact the Privacy Officer, SAOP, OGC Privacy Legal Advisor, and the other privacy officials.⁸³
- (M) At all stages of the process related to a privacy request, it is important that the Privacy Legal Advisors be kept informed to insure that this process adheres to the appropriate legal regulations.
- (N) When a request has been concluded, for whatever reason(s), the FOIA Office will send the Privacy Manager an e-mail stating that the request has been closed.

4-10. Verification of Identity. As noted above, before any documents or records can be disclosed to a requester, the Privacy Manager must verify his/her identity to assure that disclosure of any information is made to the proper person.⁸⁴ Verification can be accomplished in one of several ways:

- (A) There is no need to verify the individual's identity if the records sought are required to be disclosed to the public under FOIA, such as license files, as required by 47 CFR § 0.554 of FCC Rules. In this case, the FOIA Office will disclose the record as soon as possible.⁸⁵
- (B) If an individual makes his/her Privacy Act request in person, the requester should provide any two of the following documents to verify his/her identity.⁸⁶

Driver's License
Social Security Card
Employee Identification Card
Medicare Card
Birth Certificate
Alien Registration Card
Bank Credit Card
United States Passport
Other government-issued document (preferably with a photo ID and/or signature)

- (C) The Privacy Manager will examine the individual's documents to verify their suitability:

⁸² 47 CFR § 0.554(d); 5 U.S.C. 552a(f)(1).

⁸³ 47 CFR § 0.555(e); 5 U.S.C. 552a(f)(2), 552a(j), and 552a(k).

⁸⁴ 47 CFR §§ 0.555(a); 5 U.S.C. 552a(f)(2).

⁸⁵ 5 U.S.C. 552a(b)(2) and 552a(t); 47 CFR § 0.554(b)(3) Note.

⁸⁶ 47 CFR §§ 0.554(b)(1) and 0.555(a)(3); 5 U.S.C. 552a(f)(2).

- (1) Documents incorporating a picture and/or signature of the individual should be produced, if possible.⁸⁷
- (2) Making the request in person initiates the Commission's **10 business day** notification process.⁸⁸

Note: An individual's refusal to disclose his/her Social Security Number shall not constitute cause, in and of itself, for denial of a Privacy Act request.⁸⁹

- (D) If the individual cannot provide suitable documentation for identification, the Privacy Manager will ask the requester to sign an **Identity Statement**. The Identity Statement stipulates that knowingly or willfully seeking or obtaining access to records about another person under false pretenses is punishable by a fine of up to **\$5,000**.⁹⁰
- (E) All requests for record information sent to a requester by mail or e-mail must be signed by the individual requester and must include his/her printed name, current address, telephone number (if any), and an e-mail address (if available) when they are sent back to the FCC.
- (F) The Privacy Manager will consult the OGC Legal Advisors should there be any questions or concerns about the suitability of any documents or other issues related to verifying the individual identity.
- (G) The Privacy Manager will mail a copy of the requested record(s) to the individual after we have verified his/her identity.⁹¹ The requester's identity can be confirmed in one of two ways:⁹²
 - (1) By comparing the individual's signature on the documents he/she has provided (preferably documents containing a photograph) with those in the Commission's record(s);⁹³ or
 - (2) By using other personal details in the request letter, an attached notarized identity statement, or attested document, if the record contains no signature.⁹⁴
- (H) If the record(s) contain(s) no signatures, and if positive identification cannot be made based on other information submitted, then the Privacy Officer, Privacy Legal Advisor, and System Manager will decide whether to release the record(s), based on the degree of sensitivity of the records, as explained below:⁹⁵

⁸⁷ 47 CFR §§ 0.554(b)(1) and 0.555(a)(1).

⁸⁸ 47 CFR § 0.554(d).

⁸⁹ 47 CFR § 0.554(b)(1).

⁹⁰ 47 CFR §§ 0.554(b)(1) and (b)(2).

⁹¹ 47 CFR §§ 0.554(b)(2); 5 U.S.C. 552a(f)(1) – (f)(3).

⁹² 47 CFR §§ 0.554(b)(2), 0.555(a), and 0.555(b); 5 U.S.C. 552a(f)(1) – (f)(3).

⁹³ 47 CFR § 0.554(b)(2)..

⁹⁴ 47 CFR §§ 0.554(b)(2) and 0.555(a)(3).

⁹⁵ 47 CFR §§ 0.554(b) and 0.555(a); 5 U.S.C. 552a(f)(2) – (f)(3).

- (1) If the record contains no signature and if positive identification cannot be made based on other, suitable documentation submitted by the requester, the Privacy Officer, Privacy Legal Advisor(s), and System Manager, may decide to grant access if the record's content is not sensitive.⁹⁶

In this instance, the Commission will require the requester to sign an **Identity Statement** before releasing the record(s).⁹⁷

- (2) If positive identification cannot be made on the basis of the information submitted by the requester, and if the content of the record is so sensitive that it would cause harm or embarrassment to the individual to whom the record pertains, if seen by an unauthorized person, then the B/O System Manager, SAOP, Privacy Legal Advisors, and other privacy officials may deny the request, pending the production of better identification.⁹⁸

4-11. In-person Inspection of Documents.

- (A) When an individual, who was previously approved for a visit, arrives at FCC Headquarters to inspect the records, he/she should ask the reception desk to call the Privacy Manager⁹⁹
 - (1) After registering with the security staff, the Privacy Manager will escort the individual to the Records Information Center (RIC) where the documents can be reviewed.¹⁰⁰
 - (2) The Privacy Manager will also include the information about this visit, *i.e.*, date, time, requester, record(s) viewed, etc., in this file's records, which is submitted to the FOIA Office when this FOIA case file is closed.¹⁰¹
- (B) If the requester wants another person to accompany him/her to inspect the record(s), FCC security procedures require the requester to notify the Privacy Manager before the scheduled visit.¹⁰² The second individual must:
 - (1) Bring a photo ID;¹⁰³
 - (2) Register with the security staff to gain admittance to FCC Headquarters;¹⁰⁴ and
 - (3) Sign the authorization (along with the requester) to inspect the record(s).¹⁰⁵

⁹⁶ 47 CFR §§ 0.554(b)(2) and 0.555(a)(3); 5 U.S.C. 552a(f)(2).

⁹⁷ 47 CFR § 0.554(b)(2); 5 U.S.C. 552a(i)(3).

⁹⁸ 47 CFR §§ 0.554(b)(1) and (b)(3).

⁹⁹ 47 CFR §§ 0.555(a); 5 U.S.C. 552a(d)(1) and 552a(f)(2).

¹⁰⁰ 47 CFR §§ 0.555(a); 5 U.S.C. 552a(d)(1) and 552a(f)(3).

¹⁰¹ 47 CFR §§ 0.554(b)(1) and 0.555(a)(1) – (a)(2); 5 U.S.C. 552a(c)(1), 552a(d)(1), 552a(f)(1) – (f)(3).

¹⁰² 47 CFR §§ 0.555(a)(1); 5 U.S.C. 552a(d)(1).

¹⁰³ 47 CFR § 0.555(a)(1); 5 U.S.C. 552a(d)(1).

¹⁰⁴ 47 CFR § 0.555(a)(1); 5 U.S.C. 552a(d)(1).

¹⁰⁵ 47 CFR § 0.555(a)(1); 5 U.S.C. 552a(d)(1).

4-12. **Denying Access.** The Office of the General Counsel will advise the FCC's privacy officials about whether the Commission should grant or deny access to the subject of the record(s). In making this determination, FCC Rules under 47 CFR §§ 0.555(b) and 0.555(e) provide guidance in determining whether to deny access to all or part of a record.¹⁰⁶

(A) Access by the individual can only be denied, to the extent permitted by the Privacy Act, 5 U.S.C. 552a(d) and 552a(f), for the following reasons:

- (1) When the record is in a system of records which has an **approved exemption** from the access provisions of the Act, as noted under 47 CFR § 0.561 of FCC Rules.¹⁰⁷
- (2) When the record was compiled in reasonable anticipation of a **civil action or proceeding**.¹⁰⁸
- (3) When the record is **properly classified** and cannot be declassified.¹⁰⁹
- (4) For **investigative material** compiled for law enforcement purposes.¹¹⁰
- (5) For **investigative material** compiled solely for determining suitability for federal employment or access to classified information.¹¹¹
- (6) For certain **testing or examination materials**.¹¹²
- (7) For records containing **medical information** pertaining to an individual, when in the judgment of the system manager having custody of the records after consultation with a medical doctor, access to such record information could have an adverse impact on the individual. In such cases, a copy of the record will be delivered to a medical doctor named by the individual.¹¹³
- (8) To protect the identity of a **confidential source**. This applies to information collected since September 27, 1975 only if an express guarantee was made not to reveal the source's identity, and where the record, if stripped of the source's identity, would nonetheless reveal the identity of the subject.¹¹⁴

(B) If there is a question about denying access, the Commission may consider a **partial denial** when the exemption only applies to part of the record.¹¹⁵ OGC may advise the B/O System Manager to release the parts of the record not covered by the exemption.¹¹⁶ For example, where the exemption exists only to protect the identity of confidential

¹⁰⁶ 47 CFR §§ 0.555(b), 0.555(e), and 0.561; 5 U.S.C. 552a(f)(3), 552a(j), 552a(k).

¹⁰⁷ 47 CFR §§ 0.555(b) and 0.561; 5 U.S.C. 552a(j) and 552a(k).

¹⁰⁸ 47 CFR § 0.555(d); 5 U.S.C. 552a(d)(5).

¹⁰⁹ 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(j) and 552a(k).

¹¹⁰ 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(k)(5).

¹¹¹ 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(j) and 552a(k)(2).

¹¹² 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(k)(6).

¹¹³ 47 CFR § 0.555(b)(1); 5 U.S.C. 552a(k)(5).

¹¹⁴ 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(k)(5).

¹¹⁵ 47 CFR § 0.555(b); 5 U.S.C. 552a(f)(3), 552a(j), and 552a(k).

¹¹⁶ 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(j) and 552a(k)

sources, it may be possible to grant access to that part of the record not protected by the exemption.¹¹⁷

(C) If the Commission decides to deny full access to the record:

- (1) The Commission will send the requester a letter explaining the reasons for the denial of access and advising the individual of his/her right to seek administrative review;¹¹⁸
- (2) If the letter denying access is not sent within **10 business days**, we will send the requester a letter acknowledging the Commission's receipt of this request within **10 business days** following its receipt and advising of the projected date for completing the request (*i.e.*, for determining whether the Commission will grant this request for access, deny access, or grant a partial denial of this request.).¹¹⁹

Note: Normally, each Privacy Act request should be processed and the individual notified of the search results or the Commission's determination of whether to grant (or deny) the request within **30 business days**.¹²⁰

- (3) In the event that the Commission makes a determination to deny an individual access to records pertaining to that individual for any reason, the individual requester may appeal the FCC's decision.¹²¹

4-13. Appeal of Decision to Deny Access. An individual has the right to appeal the denial of his/her access to documents requested under the Privacy Act by **administrative review** and/or **judicial review** in U.S. District Court.¹²²

- (A) The individual may seek **administrative review** of the FCC's decision to deny him/her access to records pertaining to him/her (*i.e.*, "adverse determination"). Appeals must be received within thirty (30) days of the date of the written ruling.¹²³ The individual should address his/her appeal request in writing to the Office of the General Counsel (OGC) and state specifically why the decision should be reversed.¹²⁴ Both the letter and envelope should be marked "**PRIVACY ACT – APPEAL.**"¹²⁵
- (B) Upon receipt of the appeal request:

¹¹⁷ 47 CFR § 0.555(b)(2); 5 U.S.C. 552a(k)(2) and 555a(k)(5).

¹¹⁸ 47 CFR § 0.555(e); 5 U.S.C. 552a(d)(5), 552a(f)(2), 552a(j) and 552a(k).

¹¹⁹ 47 CFR § 0.554(d) and 0.555(e); 5 U.S.C. 552a(d)(5), 552a(f)(2), 552a(j) and 552a(k).

¹²⁰ 47 CFR § 0.554(d).

¹²¹ 47 CFR § 0.555(e); 5 U.S.C. 552a(f)(4).

¹²² 47 CFR §§ 0.555(b) and 0.555(e); 5 U.S.C. 552a(d)(5), 552a(g)(1)(B), 552a(j), and 552a(k).

¹²³ 47 CFR § 0.461(j).

¹²⁴ 47 CFR §§ 0.555(e)(1); 5 U.S.C. 552a(g)(1)(B).

¹²⁵ 47 CFR §§ 0.555(e)(1); 5 U.S.C. 552a(g)(1)(B).

- (1) OGC will advise the FOIA Office about how to log-in the request and how to treat this request and all related correspondence and documentation in the proper FOIA case file;¹²⁶ and
 - (2) The Commission is obligated to respond to this appeal in writing acknowledging receipt of the request, within the **10 business day** time frame established for all access requests.¹²⁷
 - (C) OGC will inform the SAOP and other privacy officials, and the B/O of this appeal and will request that a copy of all Commission's responses and all other relevant documents as required be forwarded to OGC.¹²⁸
 - (D) OGC will notify the SAOP and other privacy officials, and the B/O concerning the individual's appeal, as provided under 47 CFR §§ 0.555(b), 0.555(e), and 0.561 of FCC Rules and 5 U.S.C. 552a(d)(1), 552a(f)(3), 552a(g)(1)(B), 552a(g)(3)(A), 552a(j), and 552a(k).¹²⁹
 - (E) If the Commission refuses this appeal for access, the individual has the option to seek **judicial review** by a U.S. District Court, pursuant to 5 U.S.C. 552a(g)(1)(B) of the Privacy Act.¹³⁰
 - (1) OGC will provide guidance to the SAOP and other privacy officials and the B/O if the individual intends to take legal action.
 - (2) OGC will also notify the SAOP and other privacy officials, the B/O, and the FOIA Office of any actions they need to take concerning this matter.
- 4-14. Requests for Amendment or Correction. An individual subject of a Privacy Act record has a right to request that information be changed in that record.¹³¹
- (A) Requests to amend a record should be addressed to the OGC Privacy Legal Advisors (who will notify the SAOP and Privacy Manager of this request) and state clearly the reasons for the change:¹³²
 - (1) Both the envelope and letter should be marked:

“PRIVACY ACT– AMENDMENT.”¹³³

¹²⁶ 5 U.S.C. 552a(c).

¹²⁷ 47 CFR § 0.554(d) and 0.555(e)(1).

¹²⁸ 47 CFR § 0.554(d) and 0.555(e)(1).

¹²⁹ 5 U.S.C 552a(d)(1), 552a(f)(3), 552a(g)(1)(B), 552a(g)(3)(A), 552a(j) and 552a(k); 47 CFR § 0.555(b), 0.555(e), and 0.561.

¹³⁰ 5 U.S.C 552a(d)(1), 552a(f)(3), 552a(g)(1)(B); 47 CFR § 0.555(e)(2).

¹³¹ 47 CFR § 0.556; 5 U.S.C. 552a(d)(2).

¹³² 47 CFR § 0.556(a)(3); 5 U.S.C. 552a(d)(2) and 552a(f)(4).

¹³³ 47 CFR § 0.556(a).

- (2) Amendment requests must be made in writing, except for very minor changes, *e.g.*, correction of typographical errors, etc.¹³⁴
 - (3) Notification of very minor changes may be made verbally and need not be processed under this section.¹³⁵
- (B) In making a request to amend or correct a file the individual requester is required to provide sufficient information and documentation for the FCC's privacy officials to verify his/her identity,¹³⁶ as is required for any privacy request, as detailed above. At a minimum, the requester's letter should contain the following information:¹³⁷
- (1) The requester's printed name, current address, and telephone number and e-mail address (if any), as required by 47 CFR §§ 0.554(b)(2) of FCC rules;¹³⁸
 - (2) A brief description of the item or items to be changed/amended and the name of the system of records which contains the record(s), so that we can locate the record(s);¹³⁹ and
 - (3) The reason for the requested change.¹⁴⁰
- (C) When OGC receives this amendment request, they will date stamp and log the request to establish the Commission's date of receipt, and notify OGC of this request.¹⁴¹
- (1) This begins the **10 business day** response period to acknowledge the amendment request.¹⁴²
 - (2) The Commission has **30 business days** to document the handling, coordination, and completion of the Privacy Act Amendment Request.¹⁴³
- (D) OGC will advise the SAOP and privacy officials, and the appropriate B/O as to how they should handle this request to change/amend the record(s).¹⁴⁴
- (E) While OGC, the B/O, and SAOP review the amendment request,¹⁴⁵ the Commission will send the requester a letter acknowledging receipt of his/her request in which the Commission may request additional information that is needed to make a determination on this request.

¹³⁴ 47 CFR § 0.556(c); 5 U.S.C. 552a(d)(2) and 552a(f)(4).

¹³⁵ 47 CFR § 0.556(a); 5 U.S.C. 552a(d)(2) and 552a(f)(4).

¹³⁶ 47 CFR § 0.556(a); 5 U.S.C. 552a(d)(2) and 552a(4).

¹³⁷ 47 CFR § 0.556(a)(1).

¹³⁸ 47 CFR § 0.556(a)(1).

¹³⁹ 47 CFR § 0.556(a)(2).

¹⁴⁰ 47 CFR § 0.556(a)(3).

¹⁴¹ 47 CFR § 0.556(a); 5 U.S.C. 552a(d)(2) and 552a(f)(4).

¹⁴² 47 CFR § 0.556(b); 5 U.S.C. 552a(d)(2) – (d)(4), and 552a(f)(4).

¹⁴³ 47 CFR § 0.556(c); 5 U.S.C. 552a(d)(2) – (d)(4), and 552a(f)(4)..

¹⁴⁴ 47 CFR § 0.556(c) – 0.556(d); 5 U.S.C. 552a(d)(2) – (d)(4), and 552a(f)(4).

¹⁴⁵ 47 CFR §§ 0.556(b) – 0.556(c); 5 U.S.C. 552a(c)(1), 552a(d)(2) – (d)(4), and 552a(f)(4).

Note: The Commission may not send a letter acknowledging receipt of this change/amendment request if the request can be reviewed, processed, and the individual notified of compliance or denial within **10 business days**.¹⁴⁶

- (F) Should the Commission determine that it may take longer than **30 business days** to decide whether to amend/correct a record, the Privacy Manager will send a second letter or an e-mail requesting an extension of time to complete this process.¹⁴⁷
- (G) The Commission should be guided by 47 CFR § 0.556(d) in determining whether to amend the record. If the Commission makes the determinations to amend the record(s), we will notify the individual in writing and alter the record(s) as specified.¹⁴⁸
- (H) OGC and the SAOP will advise the Privacy Manager and the B/O about how the Commission intends to notify all previous recipients of the information outside the FCC in writing that this record has been corrected and to document this action. All documents related to this action should be placed in the appropriate Privacy files.¹⁴⁹
- (I) If the Commission decides to deny the amendment, OGC will advise the SAOP and other privacy officials and the B/O as to how the Commission intends to notify the individual of the refusal and the reasons for it.¹⁵⁰
- (J) In the Commission's letter denying amendment, the Commission will advise the individual requester of his/her right to request **administrative review** of the decision and of the procedures for such a review under 47 CFR §§ 0.556(c) and 0.557 of FCC Rules.¹⁵¹

4-15. Appeal of Amendment Denial. Should the Commission decide to deny a request to amend or correct a record in a system of records, the requester has the right to appeal this decision to the full Commission.¹⁵²

- (A) The individual requester has **30 business days** from the date of that the Privacy Officials made their determination not to amend a record to seek further administrative review by the full Commission.¹⁵³
- (B) The requester should send his/her request for appeal in writing to the Commission. The appeal should cite the appropriate system(s) of records to which the requester was denied amend or correct a record. Any request for administrative review must:¹⁵⁴

- (1) Clearly identify the questions presented for review,¹⁵⁵ for example:

¹⁴⁶ 47 CFR §§ 0.556(b); 5 U.S.C. 552a(d)(2).

¹⁴⁷ 47 CFR §§ 0.556(c); 5 U.S.C. 552a(d)(3).

¹⁴⁸ 47 CFR §§ 0.556(c)(1)(i) – 0.556(c)(1)(ii) and 0.556(d); 5 U.S.C. 552a(d)(2) – 552a(d)(3), and 552a(f)(4).

¹⁴⁹ 47 CFR §§ 0.556(c)(1)(iii); 5 U.S.C. 552a(c)(3) – 552a(c)(4).

¹⁵⁰ 47 CFR §§ 0.556(c)(2); 5 U.S.C. 552a(d)(2)(B)(ii) and 552(a)(f)(4).

¹⁵¹ 47 CFR §§ 0.556(c) and 0.557; 5 U.S.C. 552a(d)(3), 552(a)(f)(4), and 552a(g)(1).

¹⁵² 47 CFR §§ 0.556(c)(2), 0.556(d) and 0.557; 5 U.S.C. 552a(d)(3), 552(a)(f)(4), and 552a(g)(1).

¹⁵³ 47 CFR §§ 0.557; 5 U.S.C. 552a(d)(3) and 552(a)(f)(4).

¹⁵⁴ 47 CFR §§ 0.557(a); 5 U.S.C. 552a(d)(3) and 552(a)(f)(4).

¹⁵⁵ 47 CFR §§ 0.557(a)(1); 5 U.S.C. 552a(d)(3), 552(a)(f)(4), and 552a(g)(1)(C).

- (a) Whether the record information in question is, in fact, accurate;¹⁵⁶ and/or
 - (b) Whether information subject to a request to delete is relevant and necessary to the purpose for which it is maintained, etc.¹⁵⁷
- (2) Specify with particularity why the decision reached by the Commission's privacy officials is erroneous or inequitable;¹⁵⁸ and
- (3) Clearly state how the record should be amended or corrected.¹⁵⁹
- (C) OGC will review the appeal and prepare a response, as required by 47 CFR §§ 0.555(b), 0.557, and 0.561 of FCC Rules.¹⁶⁰
- (D) The FCC will conduct an independent review of the record in controversy using the standards of review set out in 47 CFR § 0.556(d).¹⁶¹ The Commission may seek additional information as is necessary to make a determination.¹⁶²
- (E) Final administrative review of the appeal must be completed within **30 business days** from the date of the individual's request, unless the FCC Chairman determines that the Commission requires more time to review the request. In such case, the Commission will notify the individual in writing of the delay and approximately when the review should be completed.¹⁶³
- (F) OGC will inform the individual of the Commission's decision in writing and forward a copy of the response to the SAOP, other privacy officials, and the System Manager.¹⁶⁴
- (G) If the Commission determines that the record(s) should be amended, OGC will:
 - (1) Instruct the B/O System Manager how the record should be amended;¹⁶⁵ and
 - (2) Direct the Privacy Manager as to how the Commission intends to notify all previous recipients of the information outside the FCC of the amendment.¹⁶⁶
- (H) If the FCC, upon review, decides not to amend the record(s), in whole or in part, the Commission will:¹⁶⁷

¹⁵⁶ 47 CFR §§ 0.557(a)(1); 5 U.S.C. 552a(d)(3) and 552(a)(f)(4) and 552a(g)(1)(C).

¹⁵⁷ 47 CFR §§ 0.557(a)(1); 5 U.S.C. 552a(d)(3) and 552(a)(f)(4) and 552a(g)(1)(C).

¹⁵⁸ 47 CFR §§ 0.557(a)(2); 5 U.S.C. 552a(d)(3) and 552(a)(f)(4) and 552a(g)(1)(D).

¹⁵⁹ 47 CFR §§ 0.557(a)(3); 5 U.S.C. 552a(d)(3) and 552(a)(f)(4) and 552a(g)(1)(D).

¹⁶⁰ 47 CFR §§ 0.555(b), 0.555(d), 0.556(c) – 0.556(d), 0.557, and 0.561; 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁶¹ 47 CFR §§ 0.556(d) and 0.557(b); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁶² 47 CFR §§ 0.557(b); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁶³ 47 CFR §§ 0.557(b) – 0.557(d); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁶⁴ 47 CFR §§ 0.556(c) and 0.557(c) – 0.557(d); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁶⁵ 47 CFR §§ 0.556(c)(1)(i), 0.557(c); 5 U.S.C. 552a(c), 552a(d)(3) – (d)(4).

¹⁶⁶ 47 CFR §§ 0.556(c)(1)(ii), 0.557(c); 5 U.S.C. 552a(c), 552a(d)(3) – (d)(4).

¹⁶⁷ 47 CFR §§ 0.557(d); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

- (1) Notify the individual in writing of the Commission's refusal and the reasons therefore;¹⁶⁸
- (2) Advise the individual that he/she may file a concise **statement of disagreement** stating the reasons for disagreeing with the Commission's decision.¹⁶⁹
 - (a) The statement of disagreement should be signed and addressed to the System Manager having custody of the record in question;¹⁷⁰
 - (b) This statement of disagreement must appear every time the record(s) is subsequently disclosed together with, at the Commission's discretion, a summary of the reasons the Commission has refused to amend the record;¹⁷¹ and
 - (c) The Commission will provide prior recipients of the record(s) with a copy of the statement of disagreement to the extent that an accounting of such disclosures is maintained.¹⁷²
- (3) Inform the individual that he/she may seek **judicial review** of the Commission's decision in a U.S. District Court.¹⁷³
- (4) OGC will notify the SAOP and other privacy officials, and the B/O if the individual intends to take court action.¹⁷⁴

4-16. Court Order to Amend or Grant Access. OGC will litigate any case brought by a requester in court, and the Privacy Legal Advisors will inform the SAOP and the other privacy officials of the court's verdict.¹⁷⁵

- (A) OGC is responsible for all administrative matters concerning the court order.¹⁷⁶ OGC will also direct the Privacy officials, the System Manager, and the B/O as to what procedural actions they must take:¹⁷⁷
- (B) When amendment of the record is involved, OGC will advise the SAOP, and other privacy officials, and the B/O as to how to amend the record(s)¹⁷⁸ in this information system and to carry out the court's direction.¹⁷⁹

¹⁶⁸ 47 CFR §§ 0.557(d)(1); 5 U.S.C. 552a(d)(3) and 552a (f)(4).

¹⁶⁹ 47 CFR §§ 0.557(d)(2); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁷⁰ 47 CFR §§ 0.557(d)(3)(i); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁷¹ 47 CFR §§ 0.557(d)(3)(ii) and 0.559; 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁷² 47 CFR §§ 0.557(d)(3)(iii); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁷³ 47 CFR §§ 0.557(d)(4); 5 U.S.C. 552a(d)(3), 552a(f)(4), and 552a(g)(1).

¹⁷⁴ 47 CFR §§ 0.557(d)(4); 5 U.S.C. 552a(d)(3) and 552a(f)(4).

¹⁷⁵ 5 U.S.C. 552a(g).

¹⁷⁶ 5 U.S.C. 552a(g).

¹⁷⁷ 5 U.S.C. 552a(g).

¹⁷⁸ 5 U.S.C. 552a(g)(2)(A).

¹⁷⁹ 5 U.S.C. 552a(g)(2)(A).

- (C) The Privacy Manager and the FOIA Office are also required, as directed by OGC, to notify all previous recipients of the information outside the FCC of the amendment, to document this action and to retain the information in the FOIA/Privacy Act case file(s).¹⁸⁰
- (D) When the court grants the requester access to the record(s), OGC will advise the SAOP and other privacy officials and the B/O as to how they should grant access.¹⁸¹

4-17. Charges. The FCC FOIA Office is responsible for the FOIA/Privacy Act fee schedule.

- (A) Copies of records made available via a Privacy Act request are **free** of charge for up to **25 pages**.¹⁸²
 - (1) Privacy Act requests that exceed 25 pages will incur a copying fee per page. For the current rate, please refer to the FCC's FOIA webpage at <http://www.fcc.gov/general/foia-0>.¹⁸³
 - (2) When the copies exceed 25 pages, the Privacy Officer may withhold transmittal of the copies until the Commission receives payment from the requester.¹⁸⁴
- (B) Individuals making requests under the Act must not be charged for search time or for the time spent evaluating records.¹⁸⁵

¹⁸⁰ 5 U.S.C. 552a(c)(4) and 552a(g)(2)(A).

¹⁸¹ 5 U.S.C. 552a(c)(4) and 552a(g)(2)(A).

¹⁸² 47 CFR § 0.555(c); 5 U.S.C. 552a(f)(5).

¹⁸³ 47 CFR §§ 0.555(c).

¹⁸⁴ 47 CFR §§ 0.555(c); 5 U.S.C. 552a(f)(5).

¹⁸⁵ 5 U.S.C. 552a(f)(5).

CHAPTER 5

PRIVACY ACT EXEMPTIONS

- 5-1. Exemption Policy. The FCC may determine that a system of records should be exempt from certain parts of the Privacy Act based on the information contained in the system as provided in the Privacy Act and FCC rules.¹ The main purpose of exemptions is to withhold access from the record subject where disclosure would:
- (A) Divulge classified information,²
 - (B) Reveal a confidential source,³
 - (C) Impair law enforcement investigative functions,⁴ or
 - (D) Compromise the objectivity of tests and examinations.⁵
- 5-2. General Exemption. The Chairman of the FCC may promulgate rules, in accordance with the requirements (including general notice) of 5 U.S.C. 553(b)(1), 553(b)(2), and 553(b)(3), 553(c), and 553(e) to exempt any system of records within the Commission from any part of 5 U.S.C. 552a except subsections 552a(b), 552a(c)(1) – (c)(2), 552a(e)(4)(A) – (4)(F), (e)(6), (e)(7), (e)(9), (e)(10), and (e)(11), and 552a(i), if the system of records is:⁶
- (A) **Classified Information**. Maintained by the Central Intelligence Agency,⁷ *e.g.*, classified information, where the record is currently and properly classified secret in the interest of national defense or foreign policy and cannot be declassified;⁸ or
 - (B) **Law Enforcement Records**. Maintained by an agency or component thereof which performs as its principle function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of:⁹
 - (1) Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;¹⁰

¹ 5 U.S.C. 552a(j) and 552a(k); 47 CFR §§ 0.555(b) and 0.561.

² 5 U.S.C. 552a(j) and 552a(k); 47 CFR §§ 0.555(b) and 0.561.

³ 5 U.S.C. 552a(j)(2), 552a(k)(5), and 552a(k)(7); 47 CFR §§ 0.555(b) and 0.561.

⁴ 5 U.S.C. 552a(j) and 552a(k)(2); 47 CFR § 0.555(b)(2); 47 CFR §§ 0.555(b) and 0.561.

⁵ 5 U.S.C. 552a(k)(6); 47 CFR § 0.555(b)(2).

⁶ 5 U.S.C. 552a(j) and 552a(k); 47 CFR § 0.561.

⁷ 5 U.S.C. 552a(j)(1).

⁸ 5 U.S.C. 552a(j) and 552a(k)(3) and (k)(5); 47 CFR § 0.555(b)(2).

⁹ 5 U.S.C. 552a(j)(2).

¹⁰ 5 U.S.C. 552a(j)(2)(A).

- (2) Information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual;¹¹ or
 - (3) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.¹²
 - (C) At the time rules are adopted under 5 U.S.C. 552a(j), the FCC is required to include in the statement as required under 5 U.S.C. 553(c), the reasons why the system of records is to be exempted from a provision of this section.¹³
- 5-3. **Specific Exemption.** The Chairman of the FCC, may promulgate rules, in accordance with the requirements (including general notice) of 5 U.S.C. 553(b)(1), 553(b)(2), and 553(b)(3), 553(c), and 553(e) to exempt any system of records within the Commission from 5 U.S.C. 552a(c)(3), 552a(d), 552a(e)(1), 552a(e)(4)(G), (4)(H), and (4)(I), and 552a(f) if the system of records is:¹⁴
- (A) **FCC Officials.** Officers and employees in the Commission’s Bureau or Office, which maintains the record, may have access if they have a need for the record in the performance of their duties, as allowed by the provisions of 5 U.S.C. 552a(b)(1).¹⁵
 - (B) **Law Enforcement Records.** Investigatory material compiled for law enforcement purposes, other than material within the scope of 5 U.S.C. 552a(j)(2), which covers the “general exemption” noted above, provided, however, that if any individual is denied any right, privilege, or benefit, to which he/she would otherwise be entitled by Federal law, or for which he/she would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.¹⁶
 - (C) **Protecting the President.** Maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18.¹⁷
 - (D) **Statistical Records Required by Law.** Required by statute to be maintained and used solely as statistical records.¹⁸

¹¹ 5 U.S.C. 552a(j)(2)(B); 47 CFR § 0.555(b).

¹² 5 U.S.C. 552a(j)(2)(C); 47 CFR § 0.555(b).

¹³ 5 U.S.C. 552a(j)(2).

¹⁴ 5 U.S.C. 552a(k).

¹⁵ 5 U.S.C. 552a(k)(1).

¹⁶ 5 U.S.C. 552a(k)(2).

¹⁷ 5 U.S.C. 552a(k)(3).

¹⁸ 5 U.S.C. 552a(k)(4).

Note: This exemption applies when the data are only used for statistics and not to make decisions on the rights, benefits, or entitlement of individuals.¹⁹

- (E) **Data to Determine Suitability, Eligibility, or Qualifications for Civil Service Employment.** Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Federal Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.²⁰
- (F) **Qualifying Tests for Civil Service Appointment or Promotion.** Testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process.²¹
- (G) **Data to Determine Armed Forces Promotability.** Evaluation material used to determine the potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.²²
- (H) At the time rules are adopted under this subsection, the Commission is required to include in the statement required under 5 U.S.C. 553(c), the reasons why the system of records is to be exempted from a provision of this section.²³

5-4. **Effect of Exemptions.** The exemptions cited above may free a system of records from any of the following parts of the Act:

- (A) 5 U.S.C. 552a(c)(3): Access to disclosure of accounting records.²⁴
- (B) 5 U.S.C. 552a(d): Individual access and amendment of records, review of refusal to amend, posting individual statement of disagreement with content of record, and access in anticipation of civil action or proceeding.²⁵
- (C) 5 U.S.C. 552a(e)(1): Restrictions on collecting information directly from the subject.²⁶

¹⁹ 5 U.S.C. 552a(k)(4) and 552a(6).

²⁰ 5 U.S.C. 552a(k)(5); 47 CFR § 0.555(b)(2).

²¹ 5 U.S.C. 552a(k)(6); 47 CFR § 0.555(b)(2).

²² 5 U.S.C. 552a(k)(7).

²³ 5 U.S.C. 552a(k).

²⁴ 5 U.S.C. 552a(c)(3) and 552a(k).

²⁵ 5 U.S.C. 552a(d) and 552a(k).

²⁶ 5 U.S.C. 552a(e)(1) and 552a(k).

- (D) 5 U.S.C. 552a(e)(4)(G), (4)(H), and (4)(I): Notification procedures, access procedures, and sources of records in the system of records notice.²⁷
- (E) 5 U.S.C. 552a(f): Agency rules on access/amendment, under 47 CFR §§ 0.554 – 0.557 of FCC Rules.²⁸

5-5. OMB Guidance. OMB notes that it is important for Federal agencies to recognize that Privacy Act exemptions are permissive. Even in the circumstances where a Federal agency is authorized to promulgate an exemption, the agency should only do so if the exemption is necessary and consistent with established policies.²⁹ Moreover:

- (A) While the Privacy Act allows Federal agencies to promulgate exemptions that apply at the system level, agencies should exempt only those records in a system of records for which the exemption is necessary and appropriate.³⁰
- (B) In cases where it is necessary to include exempt and non-exempt records in a single system of records, the agency should exempt only those records for which the exemption is necessary and appropriate.³¹
- (C) Federal agencies may not exempt any system of records from any provision of the Privacy Act until all the applicable reporting and publication requirements have been met.³²

5-6. Obtaining Exemptions. The bureaus and offices (B/O) wanting to obtain exemptions for all or part of a system of records shall:

- (A) Determine the specific exemption that applies to the system.³³
- (B) Request review and approval of the exemption in writing from the OGC. If the exemption is warranted, OGC will obtain a written statement from the Managing Director approving the exemption.³⁴

²⁷ 5 U.S.C. 552a(e)(4)(G) – (4)(I) and 552a(k); 47 CFR §§ 0.552 and 0.554;

²⁸ 5 U.S.C. 552a(f) and 552a(k); 47 CFR §§ 0.554 – 0.557.

²⁹ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

³⁰ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

³¹ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

³² OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

³³ 47 CFR §§ 0.555(b) and 0.561; 5 U.S.C. 552a(j) and 552a(k).

³⁴ 47 CFR §§ 0.555(b) and 0.561; 5 U.S.C. 552a(j) and 552a(k).

- (C) Establish through informal rulemaking pursuant to the Administrative Procedures Act, a rule exempting a system of records under 5 U.S.C. 552a(j) and 552a(k) of the Privacy Act.
- (D) This process generally requires publication of a proposed rule in the *Federal Register*, a public comment period, publication of a final rule, and adoption of the final rule.³⁵ At a minimum the FCC's Privacy Act exemption rules shall include:³⁶
 - (1) The specific name(s) of any system(s) that will be exempt pursuant to the rule (the name(s) shall be the same as the name(s) given in the relevant system of records notice(s));³⁷
 - (2) The specific provisions of the Privacy Act from which the system(s) of records is to be exempted and the reasons for the exemption;³⁸ and

Note: A separate reason need not be stated for each provision from which the system is being exempted, where a single explanation will serve to explain the entire exemption.³⁹

 - (3) An explanation for why the exemption is both necessary and appropriate.⁴⁰
- (E) In addition to promulgating a rule, it is also necessary that:⁴¹

³⁵ OMB Circular A-130, Appendix I, at 5 – 5(a)(2)(c); OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26; 47 CFR §§ 0.555(b) and 0.561; 5 U.S.C. 552a(j) and 552a(k).

³⁶ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 948, 28, 971-72 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26;

³⁷ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 948, 28, 971-72 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26;

³⁸ OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26;

³⁹ OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

⁴⁰ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26.

⁴¹ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26.

- (1) A description of the proposed new or revised exemption for the system of records must be described in a new or altered SORN;⁴² and
- (2) The SORN must also specify which type(s) of records are to be subject to which exemptions.⁴³

5-7. Document Submission Preparations. Following the Commission's adoption of the final rule exempting all or part of the records in a system of records from disclosure, the privacy manager will work with the B/O system manager and the OGC privacy legal advisors to draft the system of records notice (SORN) announcing the creation of a new or the alteration of an existing exemption for the system of records.

The draft SORN (whether it is a new SORN or the alternation/revision of an existing SORN) must be published in the *Federal Register* and submitted along with other associate documents to OMB and Congress for their review.⁴⁴

- (A) The SORN documents include:
 - (1) The draft new or altered/revised **System of Records Notice (SORN)** containing the exemption;⁴⁵ check on this and
 - (2) The **Transmittal Letter** and the **Narrative Statement**.⁴⁶ and
 - (3) A copy of the *Federal Register Notice* requesting public comment on the exemption.⁴⁷

Note: The specific composition of the SORN documents are detailed in Chapter 6.

- (B) The Commission will submit the draft rule for the proposed Privacy Act exemption together with the draft SORN documents to OMB and the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committee on Oversight and Government Reform for their preliminary review and approval prior to the SORN's publication in the *Federal Register*.⁴⁸

⁴² "Privacy Act Implementation: Guidelines and Responsibilities," 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26.

⁴³ "Privacy Act Implementation: Guidelines and Responsibilities," 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26.

⁴⁴ OMB Circular A-130, Appendix I, at 4(c)(1)(e), 5, and 5(a)(2)(c).

⁴⁵ OMB Circular A-130, Appendix I, at 4(c)(3)(c)(1); 5 U.S.C. 552a(e) and 552a(r).

⁴⁶ OMB Circular A-130, Appendix I, at 4(c)(3)(a) and 4(c)(3)(b); 5 U.S.C. 552a(r).

⁴⁷ OMB Circular A-130, Appendix I, at 4(c)(3)(c)(2); 5 U.S.C. 552a(r).

⁴⁸ "Privacy Act Implementation: Guidelines and Responsibilities," 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26.

- (C) In some cases exemption rules may also be subject to OMB's regulatory review procedures under Executive Order 12866, *Regulatory Planning and Review*,⁴⁹ and Executive Order 13563, *Improving Regulation and Regulatory Review*.⁵⁰
- (D) Where OMB's regulatory review is required, OMB/OIRA will notify the Commission regarding the appropriate review process, which generally means that OMB's review will require additional review time.⁵¹
- (E) Upon OMB and Congress's initial completion of its review, approval, and notification to the Commission, the privacy manager will submit the draft SORN to the Office of the Secretary for publication in the *Federal Register*.⁵²
- (F) Publication of the SORN in the Federal Register begins the **40 day public review and comment period**,⁵³ unless the Commission is seeking approval under "expedited review."⁵⁴
- (G) Running concurrent with this 40 day review is the **30 day review period** for soliciting public comments. The additional 10 days are to give OMB and Congress in which to review any public comments, if any.⁵⁵
- (H) The Commission may seek OMB approval for **expedited review** of the proposed exemption, which requires only a **30 day review period** by OMB, Congress, and the public.

Note: The procedure for seeking **expedited review** for a SORN is explained in Chapter 6.

- (I) The exemption must not be used until such time as the 40 day public comment period has ended.⁵⁶
- (J) Any exemption contained in a SORN must be published as a **final rule** before it becomes effective.⁵⁷

⁴⁹ Exec. Order No. 12,866, 58 Fed Reg. 51,735 (1993), at:

http://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

⁵⁰ Exec. Order No. 13,563, 76 Fed Reg. 3,821 (2011), at:

http://www.reginfo.gov/public/jsp/Utilities/EO_13,563.pdf cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

⁵¹ OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 27.

⁵² OMB Circular A-130, Appendix I, at 4(c)(1)(e) and 4(e)

⁵³ OMB Circular A-130, Appendix I, at 4(c)(1)(e).

⁵⁴ OMB Circular A-130, Appendix I, at 4(c)(1)(e) and 4(e)

⁵⁵ OMB Circular A-130, Appendix I, at 4(c)(1)(e), 4(c)(5), 5, and 5(a)(2)(c); 5 U.S.C. 552a(r).

⁵⁶ OMB Circular A-130, Appendix I, at 5(a)(2)(c).

⁵⁷ OMB Circular A-130, Appendix I, at 4(c)(5).

- (J) Federal agencies may not withhold records under an exemption until all of these requirements (listed above) have been met.⁵⁸

5-8. Exempted Systems of Records. The FCC maintains several systems of records that are totally or partially exempt from exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act and from 47 CFR §§ 0.554 – 0.557 of FCC Rules.⁵⁹

These systems of records may be found in the FCC’s Privacy webpages at:
http://www.fcc.gov/privacy/exempt_systems:

- (A) System Name: **FCC/WTB-1, “Wireless Services Licensing Records (ULS).”** Parts of this system of records are exempt pursuant to 5 U.S.C. 552a(k)(1), (k)(2) and (k)(3) of the Privacy Act because they: (1) contain records kept on individuals who have been subjects of FCC enforcement actions; (2) are maintained as a protective service for individuals described in Section 3056 of title 18 (18 U.S.C. 3056); (3) because they are necessary for Commission employees to perform their duties; and (4) contain investigatory materials compiled solely for law enforcement purposes.⁶⁰
- (B) System Name: **FCC/WTB-2, “Violators Files.”** Compiled for the purposes of maintaining records on individuals who have been subjects of FCC field enforcement actions. Parts of this system of records are exempt because they are maintained as a protective service for individuals described in Section 3056 of title 18, and because they are necessary for Commission employees to perform their duties, pursuant to 5 U.S.C. 552a(k)(1), (2), and (3) of the Privacy Act.⁶¹ (FCC/WTB-2 has been merged into FCC/WTB-1.)
- (C) System Name: **FCC/OGC-2, “Attorney Misconduct Files.”** This system of records is exempt pursuant to 5 U.S.C. 552a(k)(2) and (3) of the Privacy Act because it is maintained for law enforcement.⁶²
- (D) System Name: **FCC/WTB-5, “Application Review List for Present or Former Licensees, Operators, or Unlicensed Persons Operating Radio Equipment Improperly.”** Parts of this system of records are exempt pursuant to 5 U.S.C. 552a(k)(2) and (3) of the Privacy Act because they embody investigatory materials compiled solely for law enforcement purposes.⁶³ (FCC/WTB-5 has been merged into FCC/WTB-1.)
- (E) System Name: **FCC/OMD-16, “Personnel Investigation Records.”** Parts of this system of records are exempt because they embody investigatory materials pursuant to 5 U.S.C. 552a(k)(2), (3), and (5) of the Privacy Act as applicable.⁶⁴

⁵⁸ OMB Circular A-130, Appendix I, at 5(a)(2)(c).

⁵⁹ OMB Circular A-130, Appendix I, at 4(c)(1)(e) and 5(a)(2)(c); 47 CFR § 0.561; 5 U.S.C. 552a(j) and 552a(k).

⁶⁰ 47 CFR § 0.561; 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3).

⁶¹ 47 CFR § 0.561; 5 U.S.C. 552a(k)(1) – (k)(3).

⁶² 47 CFR § 0.561; 5 U.S.C. 552a(k)(2) and (k)(3).

⁶³ 47 CFR § 0.561; 5 U.S.C. 552a(k)(2) and (k)(3).

⁶⁴ 47 CFR § 0.561; 5 U.S.C. 552a(k)(2), (k)(3), and (k)(5).

- (F) System Name: **FCC/OIG-1, “Criminal Investigative Files.”** Compiled for the purpose of criminal investigations. This system of records is exempt pursuant to 5 U.S.C. 552a(j)(2) of the Privacy Act because the records contain investigatory material composed for criminal law enforcement purposes.⁶⁵ (FCC/OIG-1 has been merged into FCC/OGC-3.)
- (G) System Name: **FCC/OIG-2, “General Investigative Files.”** Compiled for law enforcement purposes. This system of records is exempt pursuant to 5 U.S.C. 552a(k)(2) of the Privacy Act because the records contain investigatory material composed for criminal law enforcement purposes.⁶⁶ (FCC/OIG-2 has been merged into FCC/OGC-3.)
- (G) System Name: **FCC/EB-5, “Enforcement Bureau Activity Tracking System (EBATS).”** Compiled for purposes of maintaining records on individuals who have been subjects of FCC enforcement actions. Parts of this system of records are exempt because they are maintained as a protective service for individuals described in Section 3056 of title 18, and because they are necessary for Commission employees to perform their duties pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(3) of the Privacy Act purposes.⁶⁷
- (H) System Name: **FCC/OIG-3, “Investigative Files.”** Compiled for the purposes of: (1) criminal investigations. This system of records is exempt pursuant to 5 U.S.C. 552a(j)(2) of the Privacy Act because the records contain investigatory material composed for criminal law enforcement purpose;⁶⁸ and (2) law enforcement purposes.⁶⁹ This system of records is exempt pursuant to 5 U.S.C. 552a(k)(2) of the Privacy Act because the records contain investigatory material composed for criminal law enforcement purposes.⁷⁰

⁶⁵ 47 CFR § 0.561; 5 U.S.C. 552a(j)(2)

⁶⁶ 47 CFR § 0.561; 5 U.S.C. 552a(j)(2).

⁶⁷ 47 CFR § 0.561; 5 U.S.C. 552a(j)(2).

⁶⁸ 47 CFR § 0.561; 5 U.S.C. 552a(j)(2).

⁶⁹ 47 CFR § 0.561; 5 U.S.C. 552a(k)(2).

⁷⁰ 47 CFR § 0.561; 5 U.S.C. 552a(k)(2).

CHAPTER 6

NEW, REVISED (ALTERED), OR CANCELLED SYSTEMS OF RECORDS

6-1. Policy. The Privacy Act at 5 U.S.C. 552a(e), requires that each electronic information system or database or collection of paper files and documents maintained by the FCC, which contains PII, must be evaluated to determine if it constitutes a **system of records**.¹

- (A) All systems of records maintained by the FCC must be covered by a **system of records notice** (SORN).
- (B) The actions to create a new SORN or to alter (revise) an existing SORN require the B/O that maintains the system of records to notify the Privacy Manager and the OGC Legal Advisors to begin this process.
- (C) In general, a B/O should not begin to operate a new or altered system of records, *i.e.*, to collect and use the PII in the system of records, until the SORN has been approved.

Note: **Chapter 5** explains the requirements for a new or altered system of records for which the Commission seeks to create an exemption from disclosure for all or part of the PII contained in the information system(s) covered by the SORN, pursuant to 5 U.S.C. 552a(j) and 552a(k) of the Privacy Act.²

6-2. Policy Guidelines. Consistent with the Privacy Act and OMB requirements, the FCC's policies governing its systems of records are to:³

- (A) Maintain in the Commission's records only that information about an individual (*i.e.* PII) as is relevant and necessary to accomplish a purpose of the Commission required to be accomplished by statute or Executive Order of the President.⁴
- (B) Collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.⁵
- (C) Provide a **Privacy Act Statement (or Privacy Act Notice)** that informs each individual whom the Commission asks to supply information about themselves on a the form, license, webpage, or other document, etc., which the Commission will use to collect the information, on the FCC website or via a hotlink to the Privacy Act Statement, or on a separate form, which can be retained by the individual.⁶

¹ 5 U.S.C. 552a(e).

² 5 U.S.C. 552a(j) and 552a(k); OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 26-27.

³ 5 U.S.C. 552a(e); OMB Circular A-108 (2016), at 5ff.

⁴ 5 U.S.C. 552a(e)(1).

⁵ 5 U.S.C. 552a(e)(2).

⁶ 5 U.S.C. 552a(e)(3). OMB Circular A-108 (2016), at 12; OMB Memorandum m-10-22, at 6.

Note: The **Privacy Act Statement** is explained fully, as appropriate, in Chapter 2 for forms, documents, and related materials; Chapter 12 for the FCC Website, and Chapter 13 for third party Websites.

- (D) Subject to the provisions of 5 U.S.C. 552a(e)(11), publish in the *Federal Register*, upon establishment or revision, a notice, *i.e.*, SORN, of the existence and character of the system of records.⁷
- (E) Maintain all records that are used by the Commission in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.⁸
- (F) Prior to disseminating any records about an individual to any person other than a Federal agency, unless the dissemination is made pursuant to a request under the *Freedom of Information Act* (FOIA), 5 U.S.C. 552a(b)(2), make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for Commission purposes.⁹

Note: The Commission's FOIA regulations and policies are on the FCC Internet website at: <https://www.fcc.gov/general/foia>.

- (G) Maintain no records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.¹⁰

Note: This requirement also covers information on an individual's political and religious activities.

- (H) Make reasonable efforts to serve notice on an individual when any record containing PII, on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.¹¹
- (I) Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any information system or database that contains PII that is covered by a system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.¹²
- (J) Establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of PII in records, and to protect against any anticipated or unanticipated threats or hazards to their security or integrity that could result in

⁷ 5 U.S.C. 552a(e)(4).

⁸ 5 U.S.C. 552a(e)(5).

⁹ 5 U.S.C. 552a(e)(6).

¹⁰ 5 U.S.C. 552a(e)(7).

¹¹ 5 U.S.C. 552a(e)(8).

¹² 5 U.S.C. 552a(e)(9).

substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.¹³

- (K) Post the Commission’s privacy policies in a **Privacy Act Statement** on the Commission’s principle website and on all other major entry points to the FCC’s sites as well as at any web page where the Commission collects substantial personal information from the public.¹⁴

Note: The **Privacy Act Statement** is explained fully, and where it is appropriate: in **Chapter 2** for forms, documents, and related materials; **Chapter 12** for the FCC Website, and **Chapter 13** for third party Websites.

- (L) At least 30 days prior to publication of information under 5 U.S.C. 552a(e)(4)(D) of the Privacy Act, publish in the *Federal Register* a SORN of any new use or intended use of the information in a system of records, and provide an opportunity for interested persons to submit written data, views, or arguments to the Commission.¹⁵

This SORN must follow the form and content prescribed by the Privacy Act, 5 U.S.C. 552a(e)(4)(D), and the guidelines of the Office of the Federal Register and OMB Circular A-108.¹⁶

Note: As noted in Section 6-7 (below), Federal agencies are now required to submit the draft SORN and the accompanying documents to OMB and the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committee on Oversight and Government Reform for their preliminary review and approval prior to the SORN’s publication in the *Federal Register*.¹⁷

- (M) Publish a notice in the *Federal Register* to note the establishment or revision of a matching agreement in which the Commission is a recipient agency or a source agency in a matching program with a **non-Federal agency**. This notice must appear at least **30 days** prior to the commencement of the matching program by the Commission.¹⁸

Note: The matching agreement notice should reference the SORN under which the FCC maintains the PII.¹⁹ **Matching Activities** are disclosed in **Chapters 10** and **11**.

¹³ 5 U.S.C. 552a(e)(10).

¹⁴ OMB Memorandum M-99-18, *Privacy Policies on Federal Web Sites*, June 2, 1999, at 1; OMB Memorandum M-05-04, at 1-2; OMB Memorandum M-10-22, Attachment A, at 7; OMB Circular A-108 (Draft 2015), at 30-31.

¹⁵ 5 U.S.C. 552a(e)(11); OMB Circular A-130, Appendix I, at 4c., 4e, 5, and 5a.

¹⁶ 5 U.S.C. 552a(e)(11); NARA, *Federal Register Document Drafting Handbook*, Section 3.12 “Privacy Act documents,” at 3-23; OMB Circular A-108 (Draft 2015), at 5-6.

¹⁷ “Privacy Act Implementation: Guidelines and Responsibilities,” 40 Fed. Reg. 28, 971 (July 9, 1975), at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, as cited in OMB Circular A-108 (draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 13-14.

¹⁸ 5 U.S.C. 552a(e)(12); OMB Circular A-130, Appendix I, at 4d, 4e., 5, and 5b; OMB Circular A-108, at 18-20.

¹⁹ 5 U.S.C. 552a(e)(12); OMB Circular A-130, Appendix I, at 4d, 4e., 5, and 5b; OMB Circular A-108, at 18-20.

6-3. New or Altered SORN.

- (A) A **new** system of records is one for which a notice (*i.e.*, a system of records notice or SORN) that has not been published in the *Federal Register*.²⁰
 - (B) A **cancelled** system of records may only be reused by publishing it in the *Federal Register* as a new SORN with a new SORN number (*i.e.*, its old number cannot be reused).²¹
 - (C) The *Federal Register Document Drafting Handbook*, Section 3.12 “Privacy Act documents,” lists **16 data elements** that must be included in a SORN in the *Federal Register*.
- Note:** Only nine of the 16 are listed under 5 U.S.C. 552a(e)(4) of the Privacy Act and FCC Rules at 47 CFR § 0.552.²²
- (D) B/O System Managers proposing new systems of records will work with the Privacy Manager and OGC Legal Advisors to compile the following information for the system notice:
 - (1) **System number.** This is the number that identifies the system of records by agency, bureau/office, and number. It is the next available number for each bureau/office.²³ For instance, if three systems exist for WTB, the system number for the new system will be “FCC/WTB-4.”
 - (2) **System name.** The name should identify the general purpose(s) of the system and, if possible, the categories of individuals involved.²⁴
 - (3) **Security classification.** The FCC’s Chief Information Officer (CIO) will evaluate the security aspects of the information system and assign an appropriate security classification level based on the guidance of the National Institutes of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), and other Federal safety and security regulation, and NARA guidelines.²⁵
 - (4) **System location(s).** Specify each address at which records are maintained in the system. If the records in a system are maintained at one or more field offices, the notice should list these locations (and in the System Manager section).²⁶

²⁰ OMB Circular A-130, Appendix I, at 4(c); 5 U.S.C. 552a(e)(4); 47 CFR § 0.552.

²¹ OMB Circular A-130, Appendix I, at 4(c).

²² NARA, *Federal Register Document Drafting Handbook*, Section 3.12 “Privacy Act documents,” at 3-23.

²³ 5 U.S.C. 552a(e)(4)(A); 47 CFR § 0.552(a); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

²⁴ 5 U.S.C. 552a(e)(4)(A); 47 CFR § 0.552(a); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

²⁵ OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

²⁶ 5 U.S.C. 552a(e)(4)(A); 47 CFR § 0.552(a); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

- (5) **Categories of individuals covered by the system.** Describe specific categories of individuals covered by the system in non-technical terms.²⁷
 - (6) **Categories of records in the system.** List the types of records maintained in the system. Include all types of records, regardless of their frequency or volume of accumulation. ~~Do not list form numbers, which may change.~~²⁸
- Note:** All forms should include the form title as well as the form number to eliminate any confusion.
- (7) **Authority for Maintenance of the System.** Cite the Federal law(s) or Executive Order(s) that authorizes maintenance of the system. Include the commonly used name of the law, where appropriate.²⁹
 - (8) **Purpose(s).** These are the objectives and uses for collecting or maintaining the information.³⁰
 - (9) **Routine Use Disclosure(s) of Records.** Routine Uses are disclosures of information maintained in the system, including categories of users and the purpose(s) of such uses to third parties, to whom the Commission may disclose information contained in the system, as appropriate.³¹
 - (a) This means that the use(s), with respect to the disclosure of a record, the use of the record for a purpose that is compatible with the purpose(s) for which it was collected, *i.e.*, the specific ways or processes in which the information is employed, including the persons or organizations to whom the record may be disclosed.³²
 - (b) Routine uses are disclosures that the FCC may be make to certain officers and others outside of the FCC for specific reason(s).³³
 - (c) Routine uses include the common and ordinary uses to which records are put, and any proper and necessary uses, even if they occur infrequently.³⁴

²⁷ 5 U.S.C. 552a(e)(4)(B); 47 CFR § 0.552(b); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

²⁸ 5 U.S.C. 552a(e)(4)(C); 47 CFR § 0.552(b); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

²⁹ 5 U.S.C. 552a(e)(3)(A); 47 CFR § 0.553(b); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

³⁰ 5 U.S.C. 552a(e)(3)(B); OMB Circular A-130, Appendix I, at 4(c)(3)(b)(1); *Document Drafting Handbook*, at 3-23.

³¹ 5 U.S.C. 552a(e)(3)(C) and 552a(e)(4)(D); 47 CFR § 0.553(d); OMB Circular A-130, Appendix I, at 4(c); *Document Drafting Handbook*, at 3-23.

³² 5 U.S.C. 552a(a)(7), 552a(b), and 552a(e)(4)(D); 47 CFR § 0.551(b)(4) and 0.552(d); OMB Circular A-130, Appendix I, at 4(c)(3)(b)(5); *Document Drafting Handbook*, at 3-23.

³³ 5 U.S.C. 552a(a)(7), 552a(b), and 552a(e)(3)(C) and (e)(4)(D).

³⁴ 5 U.S.C. 552a(a)(7) and 552a(b); 47 CFR §§ 0.551(b)(4) and 0.552(d); *Document Drafting Handbook*, at 3-23; OMB Circular A-130, Appendix I, at 4(c)(3)(b)(5).

- (d) Routine uses should describe in non-technical terms:
 - (i) The purpose for which information in the system is collected;³⁵
 - (ii) Each category of user;³⁶ and
 - (iii) The specific use made of the information by each user.³⁷
- (9) **Disclosure to Consumer Reporting Agencies.** Information may be disclosed to a consumer reporting agencies in accordance with 31 U.S.C. 3711(e).³⁸
- (10) **Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System.**³⁹ This section (or heading or element) is divided into four parts:
 - (a) **Storage.** Specify the medium in which the records are maintained.⁴⁰ For example “manual, maintained in paper files,” or “automated or electronic, maintained in computer files, magnetic tapes (or disks),” or “maintained in a combination of paper documents and computer files or other automated/electronic forms.”
 - (b) **Retrievability.** Specify how the records are accessed and retrieved such as by name, SSN, or other identification number. Indicate whether a manual or computerized index is required to retrieve individual records. (Do not show non-personal identifiers.)⁴¹
 - (c) **Safeguards.** Describe what measures are taken to prevent unauthorized disclosure of the records. State the categories of personnel authorized to have immediate access. Specify system safeguards such as safes, locked cabinets, and/or rooms, and note the presence of computer security protocols and other IT safeguards, etc., but not in such detail as to compromise security.⁴²
 - (d) **Retention and Disposal.** Indicate how long the records are retained, if and when they are retired to the Federal Records Center or the National Archives or are destroyed. A reference to the B/O Records Control Schedule or NARA General Records (GRS) Schedule item number is recommended.⁴³

³⁵ 5 U.S.C. 552a(e)(3)(C) and 552a(e)(4)(D); 47 CFR §§ 0.552(d) and 0.553(d).

³⁶ 5 U.S.C. 552a(e)(3)(C) and 552a(e)(4)(D); 47 CFR §§ 0.552(d) and 0.553(d).

³⁷ 5 U.S.C. 552a(e)(3)(C) and 552a(e)(4)(D); 47 CFR §§ 0.552(d) and 0.553(d).

³⁸ 5 U.S.C. 552a(b)(12); *Document Drafting Handbook*, at 3-23.

³⁹ 5 U.S.C. 552a(e)(4)(E) and 552a(e)(10); 47 CFR § 0.552(e); NARA, *Document Drafting Handbook*, at 3-23.

⁴⁰ 5 U.S.C. 552a(e)(4)(E) and 552a(e)(10); 47 CFR § 0.552(e); *Document Drafting Handbook*, at 3-23.

⁴¹ 5 U.S.C. 552a(e)(4)(E), 552a(e)(9), and (e)(10); 47 CFR § 0.552(e); *Document Drafting Handbook*, at 3-23.

⁴² 5 U.S.C. 552a(e)(4)(E) and 552a(e)(10); 47 CFR § 0.552(e); *Document Drafting Handbook*, at 3-23.

⁴³ 5 U.S.C. 552a(e)(4)(E); 47 CFR § 0.552(e); *Document Drafting Handbook*, at 3-23.

- (11) **System Manager(s) and Address.** Give the name of the system manager in the B/O is responsible for the policies and procedures governing the system of records, including its operations, information in the system, access, and security of the system. If the information in the system is maintained in FCC facilities, *e.g.*, headquarters, laboratories, and/or field offices, this should be noted, unless it would pose safety or security issues).⁴⁴
- (12) **Notification Procedures.** Describe the Commission's procedures whereby an individual can be notified at his/her request if the system of records contains a record pertaining to him/her. The individual may:⁴⁵
 - (a) Provide the FCC address for the FCC's Privacy Manager who functions as the contact person to whom individuals should make their notification request; or
 - (b) Fill out a FOIA request at: <https://www.fcc.gov/general/foia>.

The requester should note in this request that he/she is requesting records concerning himself/herself. The FOIA Office will then forward this request to the Privacy Manager, who will contact the requester.⁴⁶
 - (b) The requester should specify any identifying information that is required to determine if there is a record on the individual in the system.⁴⁷
 - (c) If the search finds any records related to the requester, the B/O System Manager will notify the Privacy Manager, who will contact the individual requester to inquire as to how he/she wishes to obtain the record(s) by:
 - (1) In personal inspection at FCC headquarters;⁴⁸
 - (2) By mail, since the FCC no longer transfers information in a system of records to its field locations for inspection;⁴⁹ or
 - (3) By e-mail (as a scanned document).⁵⁰

⁴⁴ 5 U.S.C. 552a(e)(4)(F), 552a(e)(9), and 552a(e)(10); 47 CFR §§ 0.552(f), 0.552(g), and 0.555(a)(2); NARA, *Document Drafting Handbook*, at 3-23.

⁴⁵ 5 U.S.C. 552a(e)(4)(G) and 552a(f)(1); 47 CFR §§ 0.552(g) and 0.554(a); NARA, *Document Drafting Handbook*, at 3-23.

⁴⁶ 5 U.S.C. 552a(e)(4)(G); 47 CFR §§ 0.552(g), 0.554(a), and 0.555(a).

⁴⁷ 5 U.S.C. 552a(f)(2); 47 CFR §§ 0.554(b), and 0.555(a).

⁴⁸ 5 U.S.C. 552a(f)(2); 47 CFR §§ 0.554(a) – 0.554(b) and 0.555(a).

⁴⁹ 5 U.S.C. 552a(f)(2); 47 CFR §§ 0.554(a) – 0.554(b) and 0.555(a).

⁵⁰ 5 U.S.C. 552a(f)(2); 47 CFR §§ 0.554(a) – 0.554(b) and 0.555(a).

- (13) **Record Access Procedures.** Briefly state how individuals can obtain access to the record pertaining to them in the system.⁵¹
- (a) As in the Notification Procedures, the individual requester should contact the Privacy Manager, who functions as the contact person to whom individuals should make their notification requests. The Privacy Manager will forward to the request to the appropriate B/O System Manager for consideration of the request.⁵²
 - (b) If the information in the system is maintained at any field offices, the Privacy Manager will work with the B/O System Managers and the field offices to process this request.⁵³
- (14) **Contesting Record Procedures.** Briefly state how individuals can contest the content of records in the system which pertains to them.⁵⁴
- (a) As in the Notification Procedures, the individual requester should contact the Privacy Manager, who will work with the FOIA Office to process this request.
 - (b) The Privacy Manager will contact the OGC Legal Advisors who will provide guidance as to the appropriate measures to take, including contacting the SAOP, FOIA Offices, and the appropriate B/O System Manager for consideration of the request of an individual seeking amendment of any record(s) or information pertaining to the individual under 47 CFR §§ 0.556 – 0.557 of FCC Rules.⁵⁵
- (15) **Record Source Categories.** List the sources of information in the system of records that pertain to the categories of individuals, the categories of records, etc.⁵⁶
- (16) **Exemptions Claimed for the System.** If no exemption has been claimed, indicate “None.” If an exemption is claimed, indicate the specific subsection(s) of the Privacy Act under which it is claimed,⁵⁷ and whether all or parts of the system are exempt.

⁵¹ 5 U.S.C. 552a(e)(4)(H) and 552a(f); 47 CFR §§ 0.552(h), 0.554, and 0.555(b); NARA, *Document Drafting Handbook*, at 3-23.

⁵² 5 U.S.C. 552a(e)(4)(G); 47 CFR §§ 0.552(g), 0.554(a), and 0.555(a).

⁵³ 47 CFR §§ 0.554 and 0.555(a).

⁵⁴ 5 U.S.C. 552a(d), 552a(e)(4)(H), and 552a(f)(4); 47 CFR §§ 0.552(h), 0.556, and 0.557; NARA, *Document Drafting Handbook*, at 3-23.

⁵⁵ 5 U.S.C. 552a(d) and (f)(4); 47 CFR §§ 0.556, and 0.557.

⁵⁶ 5 U.S.C. 552a(e)(4)(I); 47 CFR § 0.552(i); *Document Drafting Handbook*, at 3-23..

⁵⁷ 5 U.S.C. 552a(j) and 552a(k); 47 CFR §§ 0.555(b) and 0.561; *Document Drafting Handbook*, at 3-23.

The “general” and “specific” exemptions permitted under the Privacy Act and the list of the FCC’s SORNs that contain exemptions is found under 47 CFR § 0.561 of FCC rules.⁵⁸

This also found at: http://www.fcc.gov/privacy/exempt_systems.⁵⁹

6-4. Systems of Records Notices (SORNs). The Privacy Act requires Federal agencies to publish descriptions of new or altered (revised) systems of records (SORNs) in the *Federal Register*, and to submit reports on these systems to OMB and the Congress.⁶⁰ A system is considered altered whenever one of the following actions occurs or is proposed:

- (A) A significant increase in the number, type, or category of individuals about whom records are maintained.⁶¹ For example, a decision to expand a system that originally covered only residents of coastal cities to cover residents of all cities nationwide would require a report. Increases attributable to normal growth should not be reported.⁶²
- (B) A change that expands the types or categories of information maintained.⁶³ For example, a personnel file that has been expanded to include medical records would require a report.
- (C) A change that alters the purpose for which the information in the system is used.⁶⁴
- (D) A change to equipment configuration (either hardware or software) that creates substantially greater access to the records in the system of records. (It is not necessary to report changes that do not decrease the existing level of security.) For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the Commission’s headquarters would require a report.⁶⁵
- (E) The addition of an exemption pursuant to 5 U.S.C. 552a(j) or 552a(k) of the Privacy Act.

Note: As explained in **Chapter 5**, in examining a rulemaking for a Privacy Act exemption as part of a report of a new or altered system of records, OMB will also review the rule under applicable regulatory review procedures and the B/O in the Commission need not make a separate submission for that purpose.⁶⁶

⁵⁸ 5 U.S.C. 552a(j) and 552a(k); 47 CFR §§ 0.555(b) and 0.561; OMB Circular A-130, Appendix I, at 4(c)(1)(e), 4(c)(5), and 5(a)(2)(c).

⁵⁹ 5 U.S.C. 552a(j) and 552a(k); 47 CFR §§ 0.555(b) and 0.561; OMB Circular A-130, Appendix I, at 4(c)(1)(e), 4(c)(5), and 5(a)(2)(c).

⁶⁰ 5 U.S.C. 552a(e)(4) and 552a(e)(11); 47 CFR §§ 0.552 – 0.553.; OMB Circular A-130, Appendix I, at 4(c), (5), and 5(a).

⁶¹ OMB Circular A-130, Appendix I, at 4(c)(1)(a).

⁶² OMB Circular A-130, Appendix I, at 4(c)(1)(a).

⁶³ OMB Circular A-130, Appendix I, at 4(c)(1)(b).

⁶⁴ OMB Circular A-130, Appendix I, at 4(c)(1)(c).

⁶⁵ OMB Circular A-130, Appendix I, at 4(c)(1)(d).

⁶⁶ OMB Circular A-130, Appendix I, at 4(c)(1)(e), and 5(a)(2)(c).

- (F) The addition of a routine use pursuant to 5 U.S.C. 552a(b)(3) of the Privacy Act.⁶⁷

6-5. Reports for New or Altered SORNs. OMB guidelines require that:

- (A) Agencies should follow the publication format in the NARA *Office of the Federal Register's Document Drafting Handbook* and examples of prior Commission SORN FRNs.⁶⁸

Note: **Appendix 2, Office of the Federal Register System of Records Notice (SORN) Template** provides the NARA format for publishing a SORN in the *Federal Register*.

- (C) The SORN documents should be drafted in plain language, with an appropriate level of detail to ensure that members of the public are properly informed about the character of the system of records.⁶⁹

Note: The Privacy Manager will work with the B/O system manager, and OGC Legal Advisors to prepare the requisite documents for the new or altered system of records in the B/O that will maintain the system, in consultation with the SAOP and Privacy Legal Advisors.

Such cooperation will ensure that these materials are prepared for publication in the *Federal Register* and submitted to OMB and Congress on time, so that the Commission can comply fully with the public notice requirements and Congressional and OMB review periods under the Privacy Act regulations.⁷⁰

6-6. SORN Documents. The report for a new or altered system contain three elements: **Transmittal Letter, Narrative Statement, and supporting documentation**, which includes a copy of the proposed *Federal Register* notice.⁷¹

(A) **Transmittal Letter.**

- (1) The transmittal letter should be signed by the SAOP, as the senior official responsible for the routine administration of the Privacy Act in the Commission.⁷²
- (2) The transmittal letter should also contains:
- (a) The name and telephone number of the senior official in the Office of Legislative Affairs (OLA) who is the FCC's liaison with Congress and

⁶⁷ OMB Circular A-130, Appendix I, at 4(c)(1)(f)(5), and 5(a)(2)(b).

⁶⁸ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 8; OMB Circular A-130, Appendix I, at 4(c)(3); NARA, *Document Drafting Handbook*, at 3-23.

⁶⁹ 5 U.S.C. 552a(e)(4), 552a(e)(11), and 552a(r); OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 8; *Document Drafting Handbook*, at 3-23

⁷⁰ 5 U.S.C. 552a(e)(4), 552a(e)(11), and 552a(r); OMB Circular A-130, Appendix I, at 4(c), 5, and 5(a); *Document Drafting Handbook*, at 3-23.

⁷¹ OMB Circular A-130, Appendix I, at 4(c)(3).

⁷² OMB Circular A-130, Appendix I, at 4(c)(3)(a).

OMB. This officials will contact the Privacy Manager, the B/O system manage, and the senior privacy officials, as required, concerning the Commission's responses to any questions about the system of records that Congress may raise;⁷³ or

- (b) The name and telephone number of another senior privacy official, *e.g.*, Privacy Manager, who can answer questions about this proposed system.⁷⁴
- (3) The transmittal letter should also contain:
 - (a) The assurance that the proposed system does not duplicate any existing FCC or government-wide system of records;⁷⁵ and
 - (b) The assurance that the proposed system of records complies fully with the Privacy Act and OMB policies.⁷⁶
- (4) The letter sent to OMB may also request a waiver of the **40 day review period** for OMB and the House of Representatives and the Senate if the FCC is seeking **expedited review** of this SORN. In making this waiver request, the B/O in the Commission should indicate why it cannot meet the established review period and the consequences of not obtaining the waiver.⁷⁷
 - (a) If the B/O is requesting "expedited review" of the system of records notice (SORN), the Privacy Manager, the B/O System Manager in consultation with the SAOP and OGC Privacy Legal Advisors, and other staff in the B/O with responsibility for this SORN should contact the OMB desk officer and/or the privacy officials as soon as possible (by e-mail and/or a telephone conference call) to explain the reasons for making this expedited review request in obtain OMB's consent prior to submitting the SORN package to OMB.⁷⁸
 - (b) OMB requires the B/O system manager(s) to provide sufficient evidence as justification that the 40 day comment period will impose an unnecessary hardship on the Commission's activities before it will grant the waiver and allow expedited review of the SORN.⁷⁹

- (B) **Narrative Statement.** Attach a brief narrative statement, making reference, as appropriate, to information in the supporting documentation rather than restating such information.⁸⁰ The statement should include:

⁷³ OMB Circular A-130, Appendix I, at 4(c)(3)(a); OMB Circular A-108, at 17.

⁷⁴ OMB Circular A-130, Appendix I, at 4(c)(3)(a); OMB Circular A-108, at 17.

⁷⁵ OMB Circular A-130, Appendix I, at 4(c)(3)(a); OMB Circular A-108, at 17.

⁷⁶ OMB Circular A-130, Appendix I, at 4(c)(3)(a); OMB Circular A-108, at 17.

⁷⁷ OMB Circular A-130, Appendix I, at 4(c)(3)(a) and 4(e).

⁷⁸ OMB Circular A-108, at 7

⁷⁹ OMB Circular A-108, at 7

⁸⁰ OMB Circular A-130, Appendix I, at 4(3)(b).

- (1) **System Number and Name.**⁸¹
 - (2) Describe the **purpose(s)** for which the Commission is establishing the system of records.⁸²
 - (3) Identify the **authority** under which the system of records is maintained:⁸³
 - (a) Cite the underlying specific or programmatic authority (statute or executive order) rather than an overly general authority for collecting, maintaining, and using the information rather than agency housekeeping statutes; however,⁸⁴
 - (b) When the system is being operated to support a Commission housekeeping function, *e.g.*, a car pool locator, the Commission may cite the housekeeping statute that authorizes the FCC to keep such records as necessary.⁸⁵
 - (4) Provide an evaluation of the probable or potential **effects** of the proposal on the **privacy of individuals.**⁸⁶
 - (5) Provide a brief description of the steps taken by the Commission to minimize the **risk of unauthorized access** to the records in the system, which should include an assessment of the risks and specific administrative, technical, procedural, and physical safeguards that the Commission has established to safeguard the PII in the system. (This information may come from the language in “Safeguards” section of the SORN).⁸⁷
- Note: This description should not be so specific as to jeopardize the safety and security protocols.
- (6) With respect to a record’s disclosure, explain how each proposed **routine use** of such record is compatible with the purpose(s) for which it was collected, under 5 U.S.C. 552a(a)(7) of the Privacy Act.⁸⁸

For an altered (revised) system of records, and depending upon the nature of the alteration(s) or revision(s) to the system, the section of the Narrative Statement may be limited to an explanation of any new or revised proposed routine use(s).⁸⁹

⁸¹ OMB Circular A-130, Appendix I, at 4(3)(b).

⁸² OMB Circular A-130, Appendix I, at 4(3)(b)(1).

⁸³ OMB Circular A-130, Appendix I, at 4(3)(b)(2).

⁸⁴ OMB Circular A-130, Appendix I, at 4(3)(b)(2); Circular A-108, at 17.

⁸⁵ OMB Circular A-130, Appendix I, at 4(3)(b)(2).

⁸⁶ OMB Circular A-130, Appendix I, at 4(3)(b)(3).

⁸⁷ OMB Circular A-130, Appendix I, at 4(3)(b)(4).

⁸⁸ OMB Circular A-130, Appendix I, at 4(3)(b)(5); 5 U.S.C. 552a(a)(7).

⁸⁹ OMB Circular A-130, Appendix I, at 4(3)(b)(5).

- (7) Provide **OMB Control Number(s)**, **expiration date(s)**, and **title(s)** of any **information collection requirement(s)** (e.g., forms, surveys, etc.) contained in the system of records and approved by OMB under the Paperwork Reduction Act.⁹⁰ If the request for OMB clearance is pending, simply state:
- (a) The title of the collection;⁹¹ and
 - (b) The date it was submitted for OMB clearance.⁹²
- (8) If there is no information collection associated with this SORN, the following boilerplate language may be used:

Information contained in [SORN] is not a collection of information within the meaning of 5 CFR § 1320.3 of the Paperwork Reduction Act of 1995.⁹³

(C) **Supporting Documentation.** Attach the following to the narrative report:

- (1) A copy of the new or altered system of records notice (SORN) consistent with the provisions of 5 U.S.C. 552a(e)(4). The notice must appear in the format prescribed by the Office of the Federal Register's *Document Drafting Handbook*⁹⁴.
- (a) For proposed altered systems:
 - (i) Provide a copy of the original system of records notice that was published in the *Federal Register* to ensure that reviewers can understand the changes proposed.⁹⁵
 - (ii) Provide a copy of the previously published SORN and a list of the substantive changes to the previously published version of the SORN;⁹⁶ and
 - (iii) Provide a copy of the previously published SORN that has been marked up to show the changes that are being proposed.⁹⁷
 - (b) If the sole change to an existing system of records is to add a routine use, either:
 - (i) Republish the entire SORN;⁹⁸

⁹⁰ OMB Circular A-130, Appendix I, at 4(3)(b)(6).

⁹¹ OMB Circular A-130, Appendix I, at 4(3)(b)(6).

⁹² OMB Circular A-108, at 17.

⁹³ Boilerplate language provided by OMB Privacy Officer, 2003.

⁹⁴ OMB Circular A-130, Appendix I, at 4(3)(c)(1); *Document Drafting Handbook*, at 3-23.

⁹⁵ OMB Circular A-108, at 18

⁹⁶ OMB Circular A-108, at 18

⁹⁷ OMB Circular A-108, at 18

⁹⁸ OMB Circular A-130, Appendix I, at 4c(3)(c)(1).

- (ii) Give a condensed description of the system of records;⁹⁹ or
 - (iii) Give the citation to the last full text of the notice that appeared in the *Federal Register* (FRN) and include a copy of the FRN with the submission to the chairman and ranking member of the Senate and H.R. committees on government oversight.¹⁰⁰
- (2) A copy in *Federal Register* format of any new exemption rules or changes to published rules, consistent with the provisions of 5 U.S.C. 552a(f), 552(j), or 552(k) of the Act, that the Commission proposes to issue for the new or altered system.¹⁰¹
- (D) **General Changes to Multiple Systems of Records.** When an agency makes a general change to agency programs or its IT systems that apply in a similar way to multiple systems of records, *e.g.*, moving to a cloud environment, adding the same routine use to all systems of records, the agency may submit a single, consolidated report to OMB and Congress describing the changes. However, the agency shall ensure that any changes are properly reflected in all published SORNs.¹⁰²
- (E) **Circulation Procedure.** The Privacy Manager will assemble the SORN package for senior staff sign off and the SAOP's signature.
 - (1) The SORN package will include the following:
 - (a) Transmittal Letters to the Head of the Office of Information and Regulatory Affairs (OIRA) at OMB; to the Chairman and Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committees on Oversight and Government Reform;¹⁰³
 - (b) Narrative Statement;
 - (c) Draft SORN and the *Federal Register* Notice of the previous SORN if this is a revised SORN);
 - (d) "Routing Slip" for recording approvals (sign-offs); and a
 - (e) "Background Narrative" describing the SORN's history, reason(s) for the creation or revision of the SORN, and special details, etc.
 - (2) The SORN package is then circulated for final review and sign off by the following:

⁹⁹ OMB Circular A-130, Appendix I, at 4c(3)(c)(1).

¹⁰⁰ OMB Circular A-130, Appendix I, at 4c(3)(c)(1).

¹⁰¹ OMB Circular A-130, Appendix I, at 4(c)(3)(c)(2)

¹⁰² OMB Circular A-108, at 18

¹⁰³ OMB Circular A-108, at 13.

- (a) Front Office of the B/O having responsibility for this system of records
- (b) Privacy Legal Advisors in OGC;
- (c) Bureau Chief in the Office of Legislative Affairs (OLA) because the SORN documents are being sent to the two Congressional committees;
- (d) Deputy Managing Director (DMD) or the MD's Legal Advisor in OMD;
- (e) Managing Director (MD); and
- (e) Senior Agency Official for Privacy (SAOP), who conducts the final review and signs the Transmittal Letters.

6-7. OMB and Congressional "Pre-Clearance." Under Circular A-108, each Federal agency that proposes to establish or significantly alter a system of records is to provide adequate advanced notice of any such proposal to OMB and the H.R. Committee on Oversight and Governmental Reform and the Senate Committee on Homeland Security and Governmental Affairs.

- (A) This **advanced notice** to OMB and Congress is to permit them to evaluate the probable or potential effect of such proposal (*i.e.*, SORN) on the privacy or other rights of individuals.¹⁰⁴
- (B) This advanced must be at least **40 days prior** to the maintenance of the new or altered SORN becomes effective.¹⁰⁵
- (C) OMB and Congress may have **40 days to review** any proposal, the final 30 days of the review period may run **concurrently** with publication of the SORN in the Federal Register, absent instructions to the contrary from OMB or Congress.¹⁰⁶
- (D) The **40 day review period** for OMB and Congress includes an initial 10 day advanced review period, followed by a full 30 day review period that may coincide with the SORN's Federal Register publication.¹⁰⁷
- (E) The **initial 10 day review period** is to allow OMB and Congress to perform an initial review of the proposed new or altered SORN and, if possible, to provide the Commission with the opportunity to make any changes to the SORN before publication,

¹⁰⁴ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

¹⁰⁵ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

¹⁰⁶ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

¹⁰⁷ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

i.e., to obtain “pre-clearance” for this draft SORN prior to the publication in the *Federal Register*.¹⁰⁸

- (F) Should a Federal agency have to make changes to a SORN based on comments from OMB and/or Congress after the SORN’s Federal Register (FR) publication, and the agency would be required to publish a revised version of the SORN in the FR.¹⁰⁹
- (G) Since Federal agencies cannot publish the SORN in the *Federal Register* until receiving OMB authorization, OMB suggest that an agencies may decide to delay the FR publication until the end of the full 40 day review process if the agency wishes to avoid the possibility of publishing a revised version of the SORN.¹¹⁰
 - (1) The Commission may assume that the SORN is approved when the 30 days period end, if no comments have been received from Congress, OMB, and/or the public.¹¹¹
 - (2) OMB encourages each agency to consult its OIRA desk officer to confirm the procedures for OMB review of the agency’s proposals. OIRA desk officers have the discretion to adjust the OMB review procedures based on specific circumstances.¹¹²

6-8. SORN Submissions to OMB in ROCIS.¹¹³ Federal agencies must submit their SORN packages to OMB via the ROCIS electronic filing portal for both the initial 10 (to 40 day) review period and the 40 day statutory review period.¹¹⁴

- (A) The ROCIS template at: <https://www.rocis.gov> requires the following information for each SORN submission:¹¹⁵
 - (1) Title and abstract of the new or altered SORN;
 - (2) Agency (FCC) contact, *i.e.*, Privacy Manager;
 - (3) The IT system that houses the PII covered by the SORN;
 - (4) *Federal Register* citation and citation date;

¹⁰⁸ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

¹⁰⁹ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

¹¹⁰ OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 13;

¹¹¹ OMB Circular A-108, at 13; 5 U.S.C. 552a(r).

¹¹² OMB Circular A-108, at 14.

¹¹³ ROCIS is an acronym for RISC/OIRA Consolidated Information System, which was developed to facilitate the submissions and review of regulations and other agency materials, as defined in OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 16.

¹¹⁴ OMB ROCIS Manual; OMB Circular A-108, OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, (2015 Draft) at 15-16.

¹¹⁵ OMB ROCIS Manual; OMB Circular A-108, at 16.

- (5) Related SORN Review ID(s);
 - (6) Related Regulation Identifier Number (RIN) if the SORN is related to a rulemaking; and
 - (7) Related OMB Control Number(s) for PRA information collections that collect PII covered by the SORN.
- (B) The required SORN documents submitted to be submitted in ROCIS:¹¹⁶
- (1) A copy of the SORN (Word format)
 - (2) A signed copy of the Transmittal Letter (Adobe format) to the Head of OIRA/OMB;
 - (3) The Narrative Statement (Word format);
 - (4) Any other accompanying documents.
- 6-9. SORN Publication Requirements after “Pre-clearance.” Under the new OMB guidelines, after the OMB and Congressional “pre-clearance” requirement is completed, Federal agencies must then satisfy the statutory publication and public comment periods as required under 5 U.S.C. 552a(e)(11) of the Privacy Act:¹¹⁷
- (A) The Commission must publish a notice in the *Federal Register* describing the new or altered system of records, including any new use(s) or altered use(s) of the PII in the system, and provide OMB, the H.R. and Senate committees on government oversight, and the public with an opportunity in which to review the proposed SORN and to submit written data, views, or arguments to the Commission.¹¹⁸
 - (B) The reports (SORN package) must be transmitted at least **40 days** prior to the operation of the new system of records or the date on which the alteration to an existing system takes place, thereby giving OMB and the lawmakers time for further evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals,¹¹⁹ unless the Commission requests “expedited review” for the SORN.¹²⁰
 - (1) The public has a **30 day** comment period following publishing of the notice in the *Federal Register* in which to review the proposed SORN and to submit written data, views, or arguments to the Commission and OMB.¹²¹

¹¹⁶ OMB ROCIS Manual; OMB Circular A-108, at 16.

¹¹⁷ OMB Circular A-130, Appendix I, at 4(c) and 4(c)(5); 5 U.S.C. 552a(e)(11).

¹¹⁸ OMB Circular A-130, Appendix I, at 4(c) and 4(c)(5); 5 U.S.C. 552a(e)(11).

¹¹⁹ OMB Circular A-130, Appendix I, at 4(c) and 4(c)(5).

¹²⁰ OMB Circular A-108, at 13; 5 U.S.C. 552a(r).

¹²¹ OMB Circular A-130, Appendix I, at 4(c) and 4(c)(5); 5 U.S.C. 552a(e)(11).

- (2) OMB and the two Congressional committees may use the additional 10 days following the end of the 30 public comment period (in the 40 day period) in which to review and evaluate any comments that the public may submit.¹²²

Note: The Commission may request **expedited review** for the SORN, as explained in Section.¹²³

- (3) Even after completion of the “pre-clearance” review period, OMB and Congress may provide comments at any time over this 40 day review period, as required under 5 U.S.C. 552a(r) of the Privacy Act.¹²⁴
 - (3) If an agency needs to make changes to a SORN based on comments from OMB or Congress after the SORN has been published in the Federal Register, the agency will be required to publish a revised version of the SORN. There is no comment period after re-publication, and the SORN then becomes effective.¹²⁵
- (C) OMB permits the Commission to publish system of records, routine use notices, and proposed exemption rules in the *Federal Register* at the same time that the Commission sends the new or altered system(s) report to OMB and the Congress, assuming that OMB and Congress have not provided comments in their initial 10 day review period, as noted above.¹²⁶
- (1) The period for OMB, Congressional, and public review and the notice and comment period for routine uses and exemptions will then run concurrently.¹²⁷
 - (2) However, any **exemptions** (under 5 U.S.C. 552a(j) and 552a(k)) for a SORN must be published as **final rules** before they are effective, as discussed in Chapter 5.¹²⁸

Because, time periods are effective from the date the SAOP signs the Transmittal Letter to OMB and Congress (as modified by the new OMB requirements), OMB reminds Federal agencies that they should ensure these letters are transmitted expeditiously after they are signed.¹²⁹

6-10. Expedited Review.

- (A) The Head of OIRA at OMB may grant a **waiver** of the **40 day review period** for OMB and Congressional review of the proposed new or altered systems of records.¹³⁰

¹²² OMB Circular A-130, Appendix I, at 4(c) and 4(c)(5).

¹²³ OMB Circular A-108, at 13; 5 U.S.C. 552a(r).

¹²⁴ OMB Circular A-108, at 13; 5 U.S.C. 552a(r).

¹²⁵ OMB Circular A-108, at 13; 5 U.S.C. 552a(r).

¹²⁶ OMB Circular A-130, Appendix I, at 4(c)(5); 5 U.S.C. 552a(j), 552a(k), and 552a(r).

¹²⁷ OMB Circular A-130, Appendix I, at 4(c)(5); OMB Circular A-108, at 13.

¹²⁸ OMB Circular A-130, Appendix I, at 4(c)(5); 5 U.S.C. 552a(j) and 552a(k); 47 CFR § 0.561.

¹²⁹ OMB Circular A-130, Appendix I, at 4(c)(4); OMB Circular A-108, at 13-14.

¹³⁰ OMB Circular A-130, Appendix I, at 4(c)(4); OMB Circular A-108, at 16.

- (1) The B/O should discuss this request with Privacy Manager, SAOP, and OGC Privacy Legal Advisors as soon as possible, so that the OMB Desk Officer can be notified of this request and arrange for the B/O to provide the desk officer with the B/O's reasons for making this request. (Typically, OMB will require either an e-mail and/or a conference call to discuss this request.)¹³¹
- (2) The Commission must also ask for the waiver in the transmittal letter and demonstrate compelling reasons, *i.e.*, providing the formal justification for what was discussed in the e-mail and/or conference call for this waiver—typically the transmittal letter refers to this earlier discussion and the B/O's justification for the “expedited review” waiver.¹³²
- (B) When a waiver is granted, the Commission is **not** thereby relieved of any other requirement in the Act.¹³³
- (C) If no waiver is granted, the B/O in the Commission may presume concurrence at the expiration of the **40 day review period** if OMB has not commented by that time.¹³⁴
- (D) OMB cannot waive time periods specifically established by the Act such as the **30 day public comment period** following publication of the *Federal Register* notice required for the adoption of a routine use proposal pursuant to 5 U.S.C. 552a(b)(3) of the Privacy Act..¹³⁵

6-11. Cancelled Systems of Records.

- (A) Federal agencies are required to publish notices in the *Federal Register* describing altered systems of records, including the **cancellation** of any existing FCC system of records, and to submit reports to OMB, to the Chair and Ranking Member of the H.R. Committee on Oversight and Government Reform, and to the Chair and Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs.¹³⁶
- Note:** Following the effective date for a SORN that is consolidating two or more existing systems of records, the FCC will publish a such notice in the Federal Register announcing that the Commission has now cancelled these systems.¹³⁷
- (B) **Cancellation** of any existing FCC system of records shall be initiated by or coordinated with the appropriate B/O System manager, the Privacy Manager, and the OGC Privacy Legal Advisors. The proposed cancellation must be reported in writing to the Privacy Manager, Privacy Legal Advisors, and SAOP and other senior privacy officials.¹³⁸

¹³¹ OMB Circular A-130, Appendix I, at 4(c)(4); OMB Circular A-108, at 16.

¹³² OMB Circular A-130, Appendix I, at 4(c)(4); OMB Circular A-108, at 16.

¹³³ OMB Circular A-130, Appendix I, at 4(e); OMB Circular A-108, at 16.

¹³⁴ OMB Circular A-130, Appendix I, at 4(e).

¹³⁵ OMB Circular A-130, Appendix I, at 4(e); 5 U.S.C. 552a(e)(11).

¹³⁶ OMB Circular A-130, Appendix I, at 4(c)(4); 5 U.S.C. 552a(e)(4)(D), 552a(e)(11), and 552a(r); 47 CFR § 0.552; OMB Circular A-108, at 8.

¹³⁷ OMB Circular A-130, Appendix I, at 4(c)(3)(a); 5 U.S.C. 552a(r); OMB Circular A-108, at 8.

¹³⁸ OMB Circular A-130, Appendix I, at 4(c)(1)(c); OMB Circular A-108, at 8; 5 U.S.C. 552a(r).

- (C) The **transmittal letter** should be signed by the SAOP, as the agency's senior privacy official, responsible for implementation of all the Commission's Privacy Act requirements.¹³⁹
- (D) The transmittal letter should contain the name and telephone number of the individual who can best answer questions about the system of records.¹⁴⁰
- (E) The letter should also cite the reasons for the cancellation and the effective date.¹⁴¹

¹³⁹ OMB Circular A-130, Appendix I, at 4(c)(3)(a); OMB Circular A-108, at 8.

¹⁴⁰ OMB Circular A-130, Appendix I, at 4(c)(3)(a); OMB Circular A-108, at 8.

¹⁴¹ OMB Circular A-130, Appendix I, at 4(c)(3)(a); 5 U.S.C. 552a(r); OMB Circular A-108, at 8. .

CHAPTER 7

EMPLOYEE PERFORMANCE RECORDS MAINTAINED BY SUPERVISORS

- 7-1. Policy. It is important for supervisors in the B/Os to be cognizant of the FCC's records management practices that detail a supervisor's responsibilities concerning the maintenance, safeguards, and disposal of the PII in their employees' performance records, in keeping with the requirements of the Privacy Act. These Commission records management policies are to ensure that:
- (A) Sufficient documentation exists to enable supervisors/managers to operate effectively;¹
 - (B) Only relevant and necessary records are retained, and disposed of when no longer relevant and necessary;² and
 - (C) An employee's rights under the Privacy Act to know of the existence of such records and to review them are protected.³
- 7-2. Authorities.
- (A) The *Privacy Act of 1974*, 5 U.S.C. 552a, as amended, covers PII such as performance related records.⁴
 - (B) The *Civil Service Reform Act* established the requirement for agencies to develop and implement performance appraisal plans.
 - (C) 5 CFR §293 governs the contents of employee performance files, their retention schedule, disclosure restrictions and retention periods.
 - (D) The FCC Personnel Manual, Chapter 430 provides complete information on the FCC performance appraisal process and requirements.
- 7-3. Coverage of Performance Records. The performance records for FCC employees are originated or maintained by supervisors as defined by the FCC Personnel Manual, Chapter 430 (Section 1-3). This includes most GM, GS, SES, and WG series employees.
- (A) The Office of Personnel Management (OPM) periodically publishes OPM's Government-wide SORNs in the *Federal Register*, which are the ten government-wide SORNs that cover the PII the OPM maintains covering all Federal employees. These are found at: <http://www.ofr.gov/Privacy/2011/opm>.
 - (B) Employee performance records at the job site are covered by OPM/GOVT-2, "Employee Performance File System Records" SORN.⁵

¹ 5 U.S.C. 552a(e)(9) and 552a(e)(10).

² 5 U.S.C. 552a(e)(1) and 552a(e)(5)..

³ 5 U.S.C. 552a(e)(10); 47 CFR § 0.554(a); OMB Circular A-130, at 7(f) – 7(g).

⁴ 5 U.S.C. 552a.

⁵ 65 FR 24732, 24737.

7-4. Definitions. For the purposes of this directive, the following definitions shall apply:

- (A) **Employee Performance Folder (EPF)** is a separate folder established for maintaining performance records of each employee. EPFs are maintained by the AMD-HRM in accordance with OPM rules and regulations under 5 U.S.C. 293. Since EPFs are not maintained by your supervisor, inquiries about EPFs should be directed to the office of AMD-HRM.
- (B) **Performance Work Folder (PWF)** is a working folder maintained at the work site by each employee's supervisor containing performance-related documents for the current appraisal period
- (C) **Performance Plan** is the aggregation of an employee's written job elements and performance standards.
- (D) **Interim Rating** is the performance rating given an employee who is promoted or separated prior to the end of a rating period.
- (E) **Rating of Record** is the summary rating of an employee that is required on the rating due date or at the end of an extended rating period if the employee had not been under the Performance Management System standards less than 90 days.

7-5. Performance Work Folders (PWFs) Maintained by Supervisor(s). Only performance related documents may be retained in PWFs. Examples of performance related forms and documents are listed below:

CONTENTS OF PERFORMANCE WORK FOLDER

- (A) Copy of Performance Plan.
- (B) Interim Appraisals.
- (C) Any supporting performance related documentation used by the supervisor to track individual employee performance during the appraisal period, including any synopses or extracts from items such as:
 - quality control records
 - production records
 - problem/progress reports
 - log sheets
 - workload indicators
 - notes from counseling sessions with employee
- (D) Copies of documents that were created, based upon an interim or annual performance appraisal, such as:
 - recommendations for performance related training
 - award recommendations

- letters of warning regarding performance

7-6. Maintenance Instructions for PWFs.

- (A) Appraisal documents in the PWF are only maintained for the current appraisal period. The interim appraisals are attached to the rating of record, which shall be forwarded through appropriate B/O administrative channels to HRM.
- (B) A reference copy of the completed rating of record for the previous rating period may be maintained in the PWF, although no other appraisal documentation from the previous period should be retained in the PWF.

7-7. Access to PWFs.

- (A) Supervisors/managers shall provide their employees or designated representatives with access to their PWFs upon request.
- (B) Requests from parties other than the individual or his/her designated representative, *i.e.*, Freedom of Information Act (FOIA) requests, requests made under the “routine use” provisions of the Privacy Act, or uses under the Federal Labor-Management Relations statute shall be referred to the HRM.⁶

7-8. Safeguards.

- (A) HRM employees and contractors are required to adhere to the Privacy Act’s statutes and OMB regulations, etc., that pertain to protecting, safeguarding, and assuring the confidentiality, integrity, and security of the PII that is contained in the performance records that HRM maintains.
 - (1) The information in each employee’s performance records is covered by OPM/GOV-2, government-wide system of records that HRM maintains,
 - (2) This government-wide system of records includes appropriate controls and protective measures, as established by OPM, to provide the requisite proper protections for this information both during duty and non-duty hours.⁷
- (B) HRM stores the paper documents, files, and records in file cabinets in the HRM office suite.
 - (1) The file cabinets are locked when not in use and/or at the end of the business day. Access to the file cabinets is through a card-coded main door.
 - (2) Access to these records is restricted to authorized HRM supervisors, staff, and contractors.⁸

⁶ 5 U.S.C. 552a(b)(2) and 552a(t); 5 U.S.C. 552; 47 CFR §§ 0.451, 0.453, 0.457 and 0.451, and www.fcc.gov/foia.

⁷ 5 U.S.C. 552a(e)(9), 552a(e)(10), 552a(j) and 552a(k); 5 U.S.C. 552; 47 CFR §§ 0.555(b) and 0.561; OMD Circular A-130, at 8..

⁸ 5 U.S.C. 552a(e)(9) and 552a(e)(10); 47 CFR §§ 0.555(b), OMB Circular A-130, at 8..

- (C) The electronic records, files, and data are housed in the FCC's computer network databases:
- (1) Access to these electronic files is restricted is restricted to authorized HRM supervisors, staff, and contractors, who have a need for this information as part of their duties and responsibilities;
 - (2) Authorized staff and contractors in the Information Technology (IT) division, who manage the FCC's computer network databases, also have access to these electronic files; and
 - (3) Other FCC employees and contractors may be granted access only on a "need-to-know" basis.
- (D) The FCC's computer network databases are protected by the FCC's security protocols, which include controlled access, passwords, and other safety and security features and protective measures, as required under FCC policies and NIST, FISMA, OPM, and other Federal policies, programs, and regulations. Information that is resident on the FCC's computer network databases is routinely backed-up onto magnetic tape, as required and secured at an off-site location.

7-9. Retention and Disposal. Performance records shall be retained in accordance with 5 CFR § 293.

- (A) **Performance Work Folder (EPF)**. Contents of the PWF are to be treated as supporting documentation related to the appraisal records in EPFs maintained by HRM. As such, they shall generally be destroyed no later than 1 year after issuance of the appraisal, except as provided in (C) below.
- (B) **Administrative and Judicial Review**. Where any performance related documents are needed in connection with an administrative, negotiated, quasi-judicial, or judicial proceeding, they may be retained as needed beyond the retention periods identified above.⁹
- (C) When performance records are superseded through an administrative or judicial review process, they shall be destroyed.¹⁰
- (D) **Disposal Method**. Destruction of an individual's performance appraisal records shall be in accordance with the NARA records schedule and FCC procedures for the disposal of paper documents, i.e., shredding, and erasure of electronic data, or they may be offered to the subject employee.¹¹

⁹ 5 U.S.C. 552a(e)(9) and 552a(e)(10), 552a(i), 552a(j), and 552a(k); 5 U.S.C. 552; 47 CFR §§ 0.555(b) and 0.561; OMB Circular A-130, at 8, "Policy."

¹⁰ 5 U.S.C. 552a(e)(9) and 552a(e)(10), 552a(i), 552a(j), and 552a(k); 5 U.S.C. 552; 47 CFR §§ 0.555(b) and 0.561; OMB Circular A-130, at 8, "Policy."

¹¹ 5 U.S.C. 552a(e)(9) and 552a(e)(10), 552a(i), 552a(j), and 552a(k); 5 U.S.C. 552; 47 CFR §§ 0.555(b) and 0.561; OMB Circular A-130, at 8, "Policy."

CHAPTER 8

INFORMATION SYSTEMS AND TECHNOLOGY GUIDELINES

- 8-1. Policy. The FCC's Information Technology (IT) maintains and operates the Commission's IT network operations, including the information systems, subsystems, databases that collect, store, transit, maintain, and dispose of electronic data, including PII. The Chief Information Officer (CIO), as head of IT, is responsible for establishing the appropriate policies and procedures for implementing the Privacy Act with respect to the FCC's computer network operations, databases, and associated facilities operated by the IT staff and contactors.
- 8-2. Responsibilities.
- (A) The IT supervisors, staff, and contactors and direct users of the IT network who are located in the various B/Os are responsible for adhering to this chapter.
 - (B) The B/Os are responsible for complying with the FCC computer network uses set forth by this chapter.
 - (C) IT assumes safeguard responsibility for information processed or stored on the FCC network covered by the Privacy Act while the data are physically located within IT facilities; however, IT assumes no safeguard responsibility for information managed by the system owner.
 - (D) The system owner in the B/O assumes responsibility for safeguarding and providing users with access to information systems that store or process data, *i.e.*, personally identifiable information (PII) covered by the Privacy Act. These responsibilities also include ensuring that safeguards such as, but not limited to, policies and procedures that are provided by the IT staff and service providers (*e.g.*, contractors) are properly implemented, maintained, periodically reviewed, and enforced.
- 8-3. Definitions. For the purposes of this directive, the following definitions shall apply:
- (A) **Personal Data, Personally Identifiable Information, or PII** are the data, *e.g.*, documents, files, records, and related information, etc., or collections of data that are contained in a system of records, which pertain to an individual and be retrieved by the individual's name or by some number, symbol, code, or other identifying particular assigned to the individual.¹
 - (1) The definition of PII is not anchored to any single category of information or technology. Rather, it depends upon a case-by-case assessment of the specific risk that an individual can be identified;² and

¹ 5 U.S.C. 552a(a)(4) – (a)(5); 47 CFR §§ 0.551(2) – 551(3); OMB Memorandum M-22-10, Guidance on Online Use of Web Measurement and Customization Technologies, June 25, 2010, at 4.

² 5 U.S.C. 552a(a)(4) – (a)(5); 47 CFR §§ 0.551(2) – 551(3); OMB Memorandum M-22-10, Guidance on Online Use of Web Measurement and Customization Technologies, June 25, 2010, at 4.

- (2) It is important to recognize in performing this assessment that non-PII can become PII whenever additional information is made publicly available—in any medium and from any source—that when combined with other available information, could be used to identify the individual;³ and
- (3) The intentional or unintentional disclosure of this PII would result in a potentially serious invasion of the individual’s privacy.⁴

Note: The *FCC Beach Notification Policy* explains this issue in detail at: http://intranet.fcc.gov/docs/omd/perm/policies_and_procedures/Breach%20Notification%20Policy%20Sept%202015.pdf

- (A) **System Owner** is the B/O official who is responsible for the storage, maintenance, safekeeping, and disposal of the information contained in a system of records in the B/O having custody of the data, records, or information in a system of records, which it collects, uses, stores, and maintains in order to conduct its regular business. Although the IT staff and contactors process data in systems of records from other B/Os and may serve as the physical custodian, they are not the functional owner(s) of that data in the system of records.⁵

8-4. Policy and Procedures.

(A) General.

- (1) The policies set forth in Chapter 1 apply to the normal activities of IT, its employees and supervisors, and the direct users of the IT computer network systems in the B/Os.
- (2) This discussion of the Privacy Act is divided into categories that relate to the system life cycle from development through production, data security, computer security, release, and disposal or destruction of the PII or other data.
- (3) Access and distribution of PII must be restricted to those who are authorized to have access as part of their job duties and responsibilities. Other FCC staff and officials may be given access to PII only a “need-to-know” basis, as required by their job duties and responsibilities.⁶
- (4) Methods of transmission and disposal of the PII must adhere to requirements are set forth in FCCINST 1479, *FCC Cybersecurity Policy Directive*, and related documents at: <http://intranet.fcc.gov/omd/it/security.php>.

³ 5 U.S.C. 552a(a)(4) – (a)(5); 47 CFR §§ 0.551(2) – 551(3); OMB Memorandum M-22-10, Guidance on Online Use of Web Measurement and Customization Technologies, June 25, 2010, at 4.

⁴ 5 U.S.C. 552a(a)(4) – (a)(5); 47 CFR §§ 0.551(2) – 551(3); OMB Memorandum M-22-10, Guidance on Online Use of Web Measurement and Customization Technologies, June 25, 2010, at 4.

⁵ 5 U.S.C. 552a(e), and 552a(a)(1); 47 CFR §§ 0.554(3)(c).

⁶ 5 U.S.C. 552a(b)(1), 552a(e)(9) – (e)(10), 552a(o)(1), and 552a(q); 47 CFR §§ 0.554 – 0.555.

- (5) Any Commission employee who willfully and knowingly discloses personal identifiable information (PII), including electronic records, files, and data, etc., which is protected by the Privacy Act to any person or agency not entitled to receive it shall be subject to a fine of up to **\$5,000**.⁷
- (B) Access to Systems of Records.
- (1) Access to the PII contained in a system of records is limited to:
 - (a) The IT supervisors, employees, and contractors who are involved with the operation and maintenance of the FCC's computer network databases that house the PII;⁸ and
 - (b) The system manager, employees, and contractors in the B/O who require routine use of the PII, *e.g.*, information, data, and records, etc., as part of their officially assigned duties.⁹
 - (2) An exception is that individuals have a right to obtain to the PII, *e.g.*, information, data, and records, etc., pertaining to themselves, unless this information is contained in a system of records that is exempt from disclosure under 5 U.S.C. 552a(j) or a(k) of the Privacy Act.¹⁰
 - (a) The systems of records in Chapter 4 and Chapter 5 contain the rules and regulations that apply to exemptions.
 - (b) The exempt systems of records may also be found at 47 CFR § 0.561 of the FCC rules and are displayed on the FCC Privacy Webpage at: http://www.fcc.gov/Privacy/Exempt_Systems.¹¹
 - (3) Although IT is the administrator of the FCC computer network's systems, subsystems, and databases, requests for access by individuals to PII in a SORN will be handled by the system owner in the B/O, with two exceptions:¹²
 - (a) Requests for official personnel records of **current FCC employees** are the responsibility of Human Resources Management (HRM) and should be sent to HRM, as explained in Chapter 2;¹³ and
 - (b) Requests for official personnel records of **former FCC employees** are the responsibility of the Office of Personnel Management (OPM) and should be sent to OPM for action, as explained in Chapter 2.

⁷ 5 U.S.C. 552a(i) and 552a(q); 47 CFR § 0.554(b)(1).

⁸ 5 U.S.C. 552a(b)(1), 552a(e)(9) – (e)(10).

⁹ 5 U.S.C. 552a(b)(1), 552a(e)(9) – (e)(10); 47 CFR §§ 0.551(b)(5), 0.552(g), and 0.554(c).

¹⁰ 5 U.S.C. 552a(d), 552a(f), 552a(i), 552a(k), and 552a(q); 47 CFR §§ 0.552(h), 0.554, 0.555, and 0.558.

¹¹ 47 CFR § 0.561.

¹² 5 U.S.C. 552a(d), 552a(e)(G), and 552a(f)(1) – (f)(4); 47 CFR §§ 0.552(g) – 0.552(h), 0.554(c), 0.555(b), and 0.558.

¹³ 47 CFR § 0.554(c).

- (4) The system manager for each system of records is responsible for processing the access requests of individuals who submit FOIA/Privacy Act requests to the Commission seeking information about themselves.¹⁴
- (C) Safeguarding PII in Systems of Records.
- (1) **Responsibility.** Although IT is not the system owner of most systems of records processed and stored in the FCC's computer network's systems, subsystems, and databases, IT does assume responsibility for safeguarding the PII contained in the FCC's computer network that is covered by the Commission's systems of records.¹⁵
 - (a) ITC also assumes responsibility for the proper physical release of such PII to the system manager of this system of records.¹⁶
 - (b) The system manager submits the requested information to the Privacy Analyst, who then provides it to the requester or the requester's authorized representative.¹⁷
 - (2) **"Hard Copy" or Paper Documents.** PII in "hard copy," *e.g.*, paper documents, records, and files, etc., is the direct responsibility of the system manager and his/her staff in the B/O staff who maintain this PII.¹⁸
 - (a) It is system manager's responsibility to provide a copy of the PII to those who request it, unless the information is covered by a system of records that is exempt from disclosure under 5 U.S.C. 552a(j) or a(k) of the Privacy Act, as noted above.¹⁹
 - (b) It is also the system manager's responsibility to print, process, and store the hard copy data for release.²⁰
 - (c) As such, the B/O maintaining the hard copy data must ensure compliance with other relevant FCC directives, *i.e.*, the proper storage of the hard copy data and its disposal when the data are no longer needed or are obsolete in compliance with the applicable NARA records retention and disposal schedule.²¹
 - (3) **Electronic Records, Files, and Data.** It is the responsibility of the system manager to oversee the protection of the electronic data in the systems of

¹⁴ 5 U.S.C. 552a(d) and 552a(f)(1) – (f)(4); 47 CFR §§ 0.554(c), 0.555(b), and 0.558.

¹⁵ 5 U.S.C. 552a (e)(9) – (e)(10) and 552a(o); 47 CFR §§ 0.554(c) and 0.555.

¹⁶ 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(f)(1) – (f)(4).

¹⁷ 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(4); 47 CFR §§ 0.551(b)(5), 0.554(c), and 0.555.

¹⁸ 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(4); 47 CFR §§ 0.551(b)(5), 0.554(c), and 0.555.

¹⁹ 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(4); 47 CFR §§ 0.551(b)(5), 0.554(c), and 0.555.

²⁰ 5 U.S.C. 552a(d)(1), 552a(f)(1) – (f)(4); 47 CFR §§ 0.554(c) and 0.555.

²¹ 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(o)(1); 47 CFR §§ 0.551(b)(5), 0.554(c), and 0.555

records for which he/she is responsible, including restriction of the dissemination of electronic file access codes to prevent unauthorized disclosure. IT systems and management personnel involved with the assignment of file access codes will safeguard code assignment to prohibit dissemination to personnel other than those to whom codes are assigned.²²

- (D) The FCC computer network systems, subsystems, and databases are only as secure as the access constraints imposed by the operating software, operating procedures, and operating personnel.²³
 - (1) IT computer network operators should be alert to unusual events that may indicate unauthorized attempts to access the computer or data files.²⁴
 - (2) FCC policies on appropriate use of FCC computer network databases, protection of electronic media, virus prevention and other topics are discussed in *Cyber Security Policy Directive* FCCINST 1479.5 (May, 2015) and related documents at: <http://intranet.fcc.gov/omd/it/security.php>.
- (E) B/O participation in inter-agency **data sharing arrangements** require that:
 - (1) FCC employees and contractors follow the FCC's data sharing protocols, as outlined in Chapters 10 and 11, whenever PII is being transferred outside the FCC headquarters and other facilities, including protecting all PII contained in the data that are being shared; and
 - (2) These protocols should follow the requirements of the Privacy Act and related privacy regulations, FCC security requirements, and OMB guidelines and policies, so as to avoid any possibility of a breach of PII data.²⁵

Note: Data sharing arrangements and matching activities are explained in **Chapters 10 and 11**.

- (F) Any suspected, possible, or confirmed **breach** of PII that is contained in a system of records maintained by the FCC is a violation of the Privacy Act and OMB guidelines.²⁶
 - (1) The individual who is reporting this breach should immediately notify the Security Operations Center (CSO) if it is a paper-based breach and/or the Chief Information Security Officer (CISO) if it is an electronic-based breach.
 - (2) The FCC's Agency Response Team (ART) will then take the appropriate corrective action(s) and notify US-CERT.²⁷

²² 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(o)(1); 47 CFR §§ 0.551(b)(5), 0.554(c), and 0.555.

²³ 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(o)(1).

²⁴ 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(o)(1).

²⁵ OMB Memorandum M-11-02, at 3;

²⁶ 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(o).

²⁷ OMB Memorandum M-07-16, May 2007, at CITE; 5 U.S.C. 552a(e)(9) – (e)(10) and 552a(o) [CITE]; 47 CFR §§ 0.554(c) and 0.555.

Note: The *FCC Beach Notification Policy* explains this issue in detail at:
http://intranet.fcc.gov/docs/omd/perm/policies_and_procedures/Breach%20Notification%20Policy%20Sept%202015.pdf

8-5. Processing PII Outside FCC Facilities.

- (A) Some FCC information systems may require the use of equipment or services outside the direct control of FCC, *e.g.*, another government agency or a contractor.²⁸
 - (1) In such cases when records, files, or data containing PII are involved, the B/O system manager(s) must establish written rules governing the disclosure and safeguarding of PII, which is to be used by the agency or contractor. These requirements are explained in FCCINST 1479, FCC Cybersecurity Policy Directive.
 - (2) The providing agency is any entity outside the FCC that provides, generates, manages, or administers services or equipment to be used by the FCC (user agency).²⁹
- (B) At a minimum, these rules will:
 - (1) Specify clearly that the Commission's PII requires protection in compliance with the Privacy Act;³⁰
 - (2) Limit disclosure of the PII to the absolute minimum required to meet the FCC's objectives;³¹
 - (6) Set forth any special protection or considerations required based on the nature of the PII, with additional guidance for the protection of this PII that is provided in *Cyber Security Policy Directive* FCCINST 1479.5 (May, 2015) and related documents at: <http://intranet.fcc.gov/omd/it/security.php>.
 - (3) Prescribe procedures for the secure movement of privacy files between the FCC and the providing agency;³²
 - (4) Require that any reconfiguration of FCC owned equipment be approved by the CIO, CISO, and/or CDO prior to reconfiguration;³³ and

²⁸ 5 U.S.C. 552a(e)(?) and 552a(o)(1).

²⁹ 5 U.S.C. 552a(m)(1) and 552a(o).

³⁰ 5 U.S.C. 552a(e)(9) – (e)(10), 552a(m), and 552a(o); OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 16.

³¹ 5 U.S.C. 552a(e)(9) – (e)(10), 552a(m), and 552a(o); OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 16.

³² 5 U.S.C. 552a(e)(9) – (e)(10), 552a(i)(1), 552a(m), 552a(o), and 552a(q); OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 16.

³³ 5 U.S.C. 552a(e)(9) – (e)(10), 552a(i)(1), 552a(m), 552a(o), and 552a(q); OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 16.

- (C) The providing agency will acknowledge acceptance of these rules prior to the release of any data by the FCC functional owner.³⁴
- (D) Once these rules have been established, the IT staff may act as the agent for the system owner of the PII in the B/O in order to accomplish normal processing of the PII by the outside sources. IT staff and contractors will not release privacy data files to processing facilities outside the FCC except as outlined above.³⁵

³⁴ 5 U.S.C. 552a(o) and 552a(q); OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 16.

³⁵ 5 U.S.C. 552a(e)(9) – (e)(10), 552a(o), and 552a(q) OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, at 16.

CHAPTER 9

PRIVACY IMPACT ASSESSMENTS (PIAs)

- 9-1. **Policy.** The *E-Government Act of 2002* (“E-Government Act”) makes the protection of PII a major priority for the Federal agencies in their interactions with the public and as electronic information systems and databases became increasingly ubiquitous.
- (A) The E-Government Act provides guidance to Federal agencies on how to protect the privacy of individuals when agencies:
 - (1) Use information technology (IT) to collect new information,¹ or
 - (2) Develop or buy new IT systems to handle collections of PII.²
 - (B) Agencies must also describe how they handle information that individuals provide electronically to give assurance to the public that their personal information is being protected.³
 - (C) The E-Government Act requires agencies to conduct a **Privacy Impact Assessment (PIA)** to determine the extent to which their information systems provide sufficient privacy protections when such systems collect, maintain, or disseminate the PII in an identifiable form.⁴
 - (A) These PIA requirements include:
 - (1) Conducting a PIA for information systems (including both electronic databases and paper file format systems) that contain PII and making the PIA available to the public.⁵
- Note:** The FCC’s PIAs are posted on the FCC’s Privacy Act webpage at:
<https://www.fcc.gov/general/privacy-act-information#pia>.
- (2) Posting privacy policies on the FCC’s Internet website to ensure that the public has access to the policies (and also to provide a link for B/O’s easy access);⁶
 - (3) Translating privacy policies into a standardized machine-readable format;⁷ and
 - (4) Submitting the agency’s annual Federal Information Security Management Act (FISMA) report to OMB.⁸

¹ OMB Memorandum M-03-22, Sept. 26, 2003, at 1.

² OMB Memorandum M-03-22, Sept. 26, 2003, at 1.

³ OMB Memorandum M-03-22, Sept. 26, 2003, at 1.

⁴ OMB Memorandum M-03-22, Sept. 26, 2003, at 15, citing Attachment B: Section A “Purpose,” *E-Government Act of 2002*, Pub. L. No. 107-347; Dec. 17, 2002.

⁵ OMB Memorandum M-03-22, at 2.

⁶ OMB Memorandum M-03-22, at 2.

⁷ OMB Memorandum M-03-22, at 2.

⁸ OMB Memorandum M-03-22, at 2.

Note: The FISMA reporting requirements are discussed in **Chapter 15**.

9-2. PIA Responsibilities: This PIA guidance applies to:

- (A) All executive branch department and Federal agencies and their contractors that use information technology or that operate websites for purposes of interacting with the public.⁹
- (B) Relevant cross-agency initiatives, including those that further electronic government.¹⁰

9-3. Definitions. For the purposes of this directive, the following definitions shall apply:

- (A) **Information in Identifiable Form** is any information or data in an electronic database or IT system, *e.g.*, FCC forms, or in an online data collection (on the Internet), which:¹¹
 - (1) Directly identifies an individual, *e.g.*, name, address, Social Security Number, or other identifying number or code, telephone number, e-mail address, photographs, and voice prints;¹² and/or
 - (2) Agencies use to identify specific individuals in conjunction with other data elements, *i.e.*, indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, or other descriptive elements.)¹³
- (B) **Information Technology (IT)** means (as defined in the Clinger-Cohen Act)¹⁴ any equipment, software, or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.¹⁵
- (C) **Information System** means any process of collection, maintenance, use, or dissemination of information, whether performed manually with paper records, documents, and files, or electronically through the use of information technology (IT) products or design, such as computer databases, files, and records.¹⁶
- (D) **National Security System** is (as defined in the Clinger-Cohen Act) an information system operated by the Federal Government, whose functions, operations, or uses involve:

⁹ OMB Memorandum M-03-22, at 2.

¹⁰ OMB Memorandum M-03-22, at 2.

¹¹ OMB Memorandum M-03-22 (Sept 26, 2003), at 3.

¹² OMB Memorandum M-03-22 (Sept 26, 2003), at 3.

¹³ OMB Memorandum M-03-22 (Sept 26, 2003), at 3.

¹⁴ Clinger-Cohen Act of 1996, 47 U.S.C. 11101(6).

¹⁵ OMB Memorandum M-03-22 (Sept. 26, 2003), at 3; U.S. Department of Homeland Security, Privacy Office, "Privacy Threshold Analysis (PTA)," June 10, 2010, at 2: footnotes; 40 U.S.C. 11101(6).

¹⁶ USDOJ, Office of Privacy and Civil Liberties (OPCL), "Initial Privacy Assessment (IPA) Instructions and Template, March 2010, at 1; OMB Circular A-130, Nov. 30, 2000, at 6.q.

- (1) intelligence activities;
- (2) cryptographic activities related to national security;
- (3) command and control military forces;
- (4) equipment that is an integral part of a weapon or weapon systems; or
- (5) systems critical to the direct fulfillment of military or intelligence missions.

Such systems do not include systems used for administrative and business applications, such as payroll, finance, logistics, or personnel management.¹⁷

- (E) **Privacy policy in standardized machine-readable format** means a statement about site privacy practices written in standard computer language (not English text) that can be read automatically by a web browser.¹⁸

9-4. When a PIA Is Required.

- (A) Federal agencies must conduct a PIA review when:
- (1) Developing or procuring an IT information system or project to determine whether the system will collect, maintain, or disseminate information in identifiable form from or about members of the public, *i.e.*, a B/O develops any new FCC database(s), for or about its customers, which include individuals or households;¹⁹
 - (2) Initiating, consistent with the Paperwork Reduction Act (PRA), a new electronic collection of information in identifiable form for 10 or more people (excluding agencies, instrumentalities, or employees of the Federal Government);²⁰
 - (3) Revising an existing PRA information system collection that has new or revised information collection requirements that will now affect individuals or households as one of the respondent groups or when this category is being expanded to include other categories of individuals or households;²¹ and/or
 - (4) Making substantive revisions to an existing PRA information collection that affects individuals or households as one of the respondent groups, *e.g.*, changing an FCC form from a paper filing to an electronic filing or similar action.²²

¹⁷ USDOJ, Office of Privacy and Civil Liberties (OPCL), "Initial Privacy Assessment (IPA) Instructions and Template (Marcy 2010), at 1; OMB Circular A-130 (Nov. 30, 2000), at 6.q.

¹⁸ OMB Memorandum M-03-22 (Sept. 26, 2003), at 3.

¹⁹ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²⁰ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²¹ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²² OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

- (B) PIAs are also required and/or must be updated where changes to an existing information system may create new privacy risks:²³
- (1) Conversions – when converting paper-based records to electronic systems or from one electronic information system to another, *i.e.*, from one database, operating system, or software program to another program that is more advanced or up-to-date, etc.;²⁴
 - (2) Anonymous to Non-Anonymous – when functions applied to an existing information system change anonymous information to information in identifiable form;²⁵
 - (3) Significant system management changes – when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;²⁶
 - (4) Significant merging – when the FCC adopts or alters its business processes so that Commission databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated;²⁷
 - (5) New public access – when user-authenticating technology, *e.g.*, passwords, digital certificates, biometric, etc., is newly applied to an electronic information system accessed by the public;²⁸
 - (6) Commercial sources – when the FCC systematically incorporates into existing information systems, databases of information in identifiable form from commercial software, *i.e.*, commercial off-the-shelf software (COTS), or from public sources.²⁹
 - (7) New interagency uses – when the FCC works with other Federal agencies on shared functions involving significant new uses or exchanges of information in identifiable form, such as cross-cutting E-Government initiatives. (In such cases the lead agency should prepare the PIA.)³⁰
 - (8) Internal flow or collection – when alteration of a business process results in significant changes to the information that the system is collecting, using, and maintaining, *i.e.*, when the system is adds new information in identifiable form to the information that it is currently collecting, which could potentially raise personal privacy risks;³¹

²³ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²⁴ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²⁵ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²⁶ OMB Memorandum M-03-22, Sept. 26, 2003, at 3.

²⁷ OMB Memorandum M-03-22, Sept. 26, 2003, at 4.

²⁸ OMB Memorandum M-03-22, Sept. 26, 2003, at 4.

²⁹ OMB Memorandum M-03-22, Sept. 26, 2003, at 4.

³⁰ OMB Memorandum M-03-22, Sept. 26, 2003, at 4.

³¹ OMB Memorandum M-03-22, Sept. 26, 2003, at 4.

- (9) Alteration in the character of data – when new information in identifiable form is added to a collection that might raise the risks to personal privacy, *e.g.*, adding a new category of PII to a database.³²
 - (C) The B/O must revise/update an existing PIA when changes are made to information collection authorities, business processes, or other factors that significantly affect the collection and handling of PII.³³
- 9-5. When a PIA is not Required. A Federal agency is not required under the E-Government Act to conduct a PIA in these circumstances:
- (A) When the PTA (in the FCC’s policy) has determined that no PII is being collected by an information system or database;³⁴
 - (B) For FCC websites, IT systems, or information collections to the extent that they do not collect or maintain PII about members of the general public (including FCC staff and contractors);³⁵
 - (C) For those FCC websites where the user is given the option of contacting the FCC (site operator) for the limited purposes of providing feedback, *e.g.*, miscellaneous questions or comments) or obtaining additional information.³⁶
 - (D) For national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology by Section 202 of the E-Government Act.³⁷
 - (E) When all elements of a PIA are addressed in a matching agreement by the computer matching provisions of the Privacy Act, 5 U.S.C. 552a(8) – (a)(10), (e)(12), (o), (p), (q), (r), (u), which specifically provide privacy protections for matched information.³⁸
 - (F) When all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use.³⁹
 - (G) If the FCC is developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generate PII.⁴⁰

³² OMB Memorandum M-03-22, Sept. 26, 2003, at 4.

³³ OMB Memorandum M-03-22, Sept. 26, 2003, at 5.

³⁴ FCC PTA Template, Question 1.20, at 11.

³⁵ OMB Memorandum M-03-22, Sept. 26, 2003, at 5.

³⁶ OMB Memorandum M-03-22, Sept. 26, 2003, at 5.

³⁷ OMB Memorandum M-03-22, Sept. 26, 2003, at 5.

³⁸ OMB Memorandum M-03-22, Sept. 26, 2003, at 5.

³⁹ OMB Memorandum M-03-22, Sept. 26, 2003, at 6.

⁴⁰ OMB Memorandum M-03-22, Sept. 26, 2003, at 6.

- (H) For minor changes to an information system or database or PRA information collection that do not create new privacy risks.⁴¹
- (I) For a routine extension of an existing PRA information collection (even when the information collection's respondent group includes "individuals or household");⁴²
- (J) For a revision of an information collection, which affects "individuals or household," when the revision is for rules or regulations, or significant changes to an FCC form, but the changes will **not** affect the collection of information about "individuals or household" (*i.e.*, PII).⁴³

9-5. FCC's PIA Policy.

- (A) The FCC has adopted a more comprehensive policy approach in regards to how the Commission complies with the E-Government Act's PIA requirements.
- (B) The FCC uses a two-tier process for evaluating its information systems and databases, which follows the example of the U.S. Department of Justice (DOJ), the Department of Homeland Security (DHS), and several other Federal agencies:
 - (1) The first or initial review is the **Privacy Threshold Analysis (PTA)** that determines if the information system or database contains PII; and
 - (2) The second review is the more detailed **Privacy Impact Assessment (PIA)** that evaluates the privacy risks and vulnerabilities in an IT information system or database that contains PII.
- (C) The Commission has also chosen to conduct a PTA for **all** its information systems, including PII contained in both the electronic (IT) and paper document formats, rather than limiting the PTA review to those information systems meeting the minimal requirements of the E-Government Act.
- (D) The Commission adopted this comprehensive approach:
 - (1) To insure that **all** IT information systems receive the minimal PTA review; and
 - (2) To eliminate any possibility that an information system could be collecting PII without its being so identified and the proper steps being taken to evaluate the system's treatment of PII and to identify any system vulnerabilities.

9-6. Privacy Threshold Analysis (PTA). The PTA is the FCC's initial tool to identify any potential privacy issues in **all** the FCC's information systems (including both IT systems and paper document files), unless it has already been determined that the system contains PII, *e.g.*, systems for which a SORN already exists.

⁴¹ OMB Memorandum M-03-22, Sept. 26, 2003, at 6.

⁴² OMB Memorandum M-03-22, Sept. 26, 2003, at 5.

⁴³ OMB Memorandum M-03-22, Sept. 26, 2003, at 6.

- (A) The Privacy Manager conducts the PTA review with the B/O System Manager(s) and other employees and contractors who work closely with the information system and the IT and Security Office staffs, who are needed to provide knowledge, guidance, and assistance with the system’s IT and security vulnerabilities.⁴⁴
- (B) The PTA’s purposes are to determine:
 - (1) The kinds of information that the system is collecting; and
 - (2) Whether there are any privacy issues—is the system collecting PII.⁴⁵
- (C) The PTA asks a series of questions to determine:
 - (1) The status of the information system:
 - (a) Is it a new system or a revised or upgraded system;⁴⁶ and
 - (b) If it is being revised or upgraded system, what are the reasons for these system changes.⁴⁷
 - (2) The kind(s) of information that the system is collecting, storing, maintaining, and using—does this include PII;⁴⁸
 - (3) The sources for the information that is being collected;⁴⁹
 - (4) Whether the information system is a “stand alone” system or if it has “links” or “connections” to other FCC and/or non-FCC information systems that provide an avenue for the transfer or exchange of information, including PII:
 - (a) If there are linkages—what are these;⁵⁰
 - (b) What kind(s) of information is being transmitted or linked;⁵¹ and
 - (c) Are there any vulnerabilities that might include privacy concerns posed by the linkage(s);⁵²
 - (5) The risks for inadvertent disclosure of the information in the system;⁵³

⁴⁴ USDOJ, Office of Privacy and Civil Liberties (OPCL), “Initial Privacy Assessment (IPA) Instructions & Template” (Revised March 2010), at 2;

⁴⁵ USDOJ, OPCL (Revised March 2010), at 1.

⁴⁶ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 1.

⁴⁷ USDOJ, OPCL (Revised March 2010), at 1 FCC PTA Template, at 1.

⁴⁸ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 3 – 6.

⁴⁹ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 7.

⁵⁰ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 7.

⁵¹ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 7 – 8.

⁵² USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 9.

⁵³ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 10.

- (6) If the information system does include PII, is it compliant with the applicable privacy laws and OMB and FCC privacy regulations and policies;⁵⁴
- (D) If the PTA determines that the information system **does not** contains PII, the process stops.
 - (1) Then the B/O System Manager(s) and the Privacy Manager sign the Certification Statement.
 - (2) The PTA is sent to the SAOP for final review. The SAOP reviews the PTA, and signs the **Certification Statement**.
 - (3) The PTA is posted on the FCC's webpage for public review;⁵⁵ but
- (E) If the PTA determines that the information system does contains PII:
 - (1) The Privacy Manager and B/O System Manager also sign the Certification Statement.
 - (2) The PTA is sent to the SAOP for final review. The SAOP reviews the PTA, and signs the **Certification Statement**.
 - (3) The PTA is posted on the FCC's webpage for public review;⁵⁶ and
 - (4) The Privacy Manager starts the process to arrange the meeting to conduct the PIA.⁵⁷
- (F) The list of the FCC's completed PTAs may be found at:
<https://www.fcc.gov/general/privacy-act-information#pia>.
- 9-7. Privacy Impact Assessment (PIA). The **PIA** is a lengthier and more comprehensive review that evaluates, analyses, and assesses how PII in the information system is handled:
 - (A) To ensure that this handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;⁵⁸
 - (B) To determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form (*i.e.*, PII) in an electronic information system;⁵⁹

⁵⁴ USDOJ, OPCL (Revised March 2010), at 1; FCC PTA Template, at 10 – 11.

⁵⁵ FCC PTA Template, at 10 – 11.

⁵⁶ FCC PTA Template, at 10 – 11.

⁵⁷ OMB Memorandum M-03-22 (Sept. 26, 2003), at 6.

⁵⁸ OMB Memorandum M-03-22 (Sept. 26, 2003), at 4; OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010 at 8.

⁵⁹ OMB Memorandum M-03-22, Sept. 26, 2003, at 4; OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010 at 8.

- (C) To examine and evaluate protections and alternative processes for handling the information to mitigate potential risks;⁶⁰ and
- (D) To evaluate and determine how the information system treats the PII:⁶¹
 - (1) What PII is the information system collecting, (*i.e.*, kind(s) of PII data and the source(s)) of this PII;⁶²
 - (2) Why is the PII being collected;⁶³
 - (3) What are the intended uses of the PII;⁶⁴
 - (4) With whom will the PII be shared or transmitted between the information system and other FCC or non-FCC information systems and for what purpose(s);⁶⁵
 - (7) What notice or opportunities for consent do individuals have to decline to provide their PII;⁶⁶
 - (a) Is the PII collection voluntary;⁶⁷
 - (b) Did the individual consent to particular uses of the PII other than required or authorized uses of the PII;⁶⁸
 - (c) How do individuals grant consent for the use of their PII.⁶⁹
 - (8) How will the information be secured, e.g., what are the administrative and technical controls?⁷⁰
 - (9) Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?⁷¹
- (E) The FCC's PIA template also asks for other information that is deemed important to understanding the characteristics and uses of the PII in the information system:
 - (1) Who are the developers and managers of the information system?

⁶⁰ OMB Memorandum M-03-22, Sept. 26, 2003, at 4; OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010 at 8.

⁶¹ OMB Memorandum M-03-22, at 2.

⁶² OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶³ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶⁴ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶⁵ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶⁶ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶⁷ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶⁸ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁶⁹ OMB Memorandum M-03-22, at 5. FCC PIA Template.

⁷⁰ OMB Memorandum M-03-22, at 5; FCC PIA Template.

⁷¹ OMB Memorandum M-03-22, at 5; FCC PIA Template.

- (2) What impacts do the Data Quality, Utility, Objectivity and Integrity requirements have on the PII in the information system?⁷²
- (3) What training is available for those who manage the information system and for those who have access to the PII.⁷³
- (4) Are there any information collections (under the Paperwork Reduction Act) associated with this information system and its PII?⁷⁴
- (5) If the information system requires a system of records—what opportunity does an individuals have to inquire as to whether the information system contains PII about them.⁷⁵
- (6) Does this information system include a consumer satisfaction survey as part of the public access to the PII.⁷⁶
- (7) What are the potential privacy risks and vulnerabilities for the PII covered in this information system?⁷⁷

9-8. Initiating PTAs and PIAs.

- (A) The Privacy Manager and the B/O's system manager and other employees and contractors who manage the information system should initiate a PTA when:
 - (1) The B/O begins to develop a new information system;⁷⁸
 - (2) The B/O makes substantive changes to an information system, such as changes to the IT operating system or the types of information that is being collected;⁷⁹ or
 - (2) The B/O revises an existing information collection that may potentially affect individuals or households.⁸⁰
- (B) At the IT development stage, when the PTA has determined that the information system will collect PII, the PIA will address:

⁷² FCC PIA Template, at Section 4.0.

⁷³ OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, at 6; FCC PIA Template.

⁷⁴ OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, at 6; FCC PIA Template.

⁷⁵ OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, at 6; FCC PIA Template.

⁷⁶ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁷⁷ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁷⁸ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁷⁹ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁰ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

- (1) The privacy issues related to systems development, including, as warranted and appropriate, the statement of need, functional requirements analysis, alternative analysis, feasibility analysis, cost-benefits analysis, and especially, initial risk assessment.⁸¹
- (2) The impact the system will have on an individual's privacy (at this stage of development), specifically identifying and evaluating the potential threats relating to:⁸²
 - (a) The type(s) of PII to be collected;⁸³
 - (b) The reason(s) for collecting the PII;⁸⁴
 - (c) The proposed uses for the PII;⁸⁵
 - (d) With whom the PII may be shared;⁸⁶
 - (e) The opportunities for individuals to decline to provide their PII;⁸⁷
 - (f) The safeguards to protect and secure the PII;⁸⁸ and
 - (g) Whether a system of records being created or revised.⁸⁹
- (3) Later reevaluation or reappraisal of the privacy impact(s) as the information system is developed to consider issues not identified earlier in IT development process.⁹⁰
- (C) The "information life cycle" – collection, use, retention, processing, disclosure, and destruction of the information system's PII in evaluating how information is handled at each stage that may affect an individual's privacy.⁹¹
- (D) Each PTA and PIA must be approved by the SAOP (or other senior privacy official);⁹² and
- (E) Each PTA and PIA will be posted on the FCC's privacy webpage to be made publicly available, except when the PIA would raise national security concerns, reveal classified

⁸¹ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸² OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸³ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁴ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁵ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁶ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁷ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁸ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁸⁹ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁹⁰ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁹¹ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁹² OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

or sensitive information such as national interest issues or law enforcement, and/or proprietary business or related issues and concerns.⁹³

(F) No PII should be included in a PTA or PIA.⁹⁴

9-9. PTAs and PIAs for Major Information Systems. Major information systems are large, complex information systems, with high annual or system life costs associated with their development, operations, and maintenance, and the potential for high risk or harm if the information they manage is compromised. Because of their characteristics, the PTAs and PIAs for these information systems should also evaluate:

(B) The consequences of the collections and flow of information in the system;⁹⁵

(C) Alternatives to the collection and handling of information as the system has been designed;⁹⁶

(D) Appropriate measures to mitigate risks identified for each alternative;⁹⁷ and

(E) The rationale for the final design choice or business process for the system.⁹⁸

Note: A full description of what constitutes the FCC's Major Information Systems along with a roster of these systems is at: <https://www.fcc.gov/general/privacy-act-information#major>.

9-10. Adaptive PTAs and PIAs. Adaptive PTAs and PIAs for the FCC's webpages are found in Chapters 12 and 13.

9-11. Conducting a PIA with a SORN. When it has been determined either by a PTA review or because the B/O knows in advance that an information system will include PII, the B/O may:

(A) Conduct a PIA when developing a SORN as required by 5 U.S.C. 552a(e)(4) of the Privacy Act, in that the PIA and system of records overlap in content, such as categories of records, uses for the PII, policies and procedures for handling the PII;⁹⁹

(B) Publish the PIA concurrently with the SORN covering the system of records in the Federal Register;¹⁰⁰ and

(C) Consider whether a PIA is required when altering or revising an existing SORN.¹⁰¹

⁹³ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁹⁴ OMB Memorandum M-03-22, Sept. 26, 2003, at 6; FCC PIA Template.

⁹⁵ OMB Memorandum M-03-22 (Sept. 26, 2003), at 5.

⁹⁶ OMB Memorandum M-03-22 (Sept. 26, 2003), at 5.

⁹⁷ OMB Memorandum M-03-22 (Sept. 26, 2003), at 5.

⁹⁸ OMB Memorandum M-03-22 (Sept. 26, 2003), at 5.

⁹⁹ OMB Memorandum M-03-22 (Sept. 26, 2003), at 6.

¹⁰⁰ OMB Memorandum M-03-22 (Sept. 26, 2003), at 6.

¹⁰¹ OMB Memorandum M-03-22 (Sept. 26, 2003), at 6.

9-12. Information Collection Requests (ICRs) and PIAs. OMB allows an option for a combined ICR and PIA as part of a PRA submission.¹⁰²

(A) The B/O should:

- (1) Notify the Privacy Manager of this requirement,¹⁰³ and
- (2) Submit the PIA at the same time as the information collection.¹⁰⁴

(B) The PERM PRA reviewers will review the PIA along with the PRA submission and forward both the PIA and ICR documents to OMB.¹⁰⁵

(C) The PRA representative should include all the elements of the PIA within the structure of the Supporting Statement of the information collection. The elements must be addressed clearly and be easily identifiable.¹⁰⁶

(D) The PIA elements are as follows:

- (1) A description of the information (on individuals or households) to be collected in the response to Item 1 of the Supporting Statement.¹⁰⁷
- (2) A description of how the information (on individuals or households) will be shared and for what purpose in Item 2 of the Supporting Statement.¹⁰⁸
- (3) A statement detailing the impact(s) the proposed collection will have on privacy in Item 2 of the Supporting Statement.¹⁰⁹
- (4) A discussion in Question 10 of the Supporting Statement of:
 - (a) Whether the individuals are informed that providing the information is mandatory or voluntary;¹¹⁰
 - (b) Opportunities to consent, if any, to sharing and submission of information;¹¹¹
 - (c) How the information (on individuals or households) will be secured;¹¹² and

¹⁰²

¹⁰³

¹⁰⁴

¹⁰⁵

¹⁰⁶

¹⁰⁷

¹⁰⁸ OMB Memorandum M-03-22, at 6.

¹⁰⁹ OMB Memorandum M-03-22, at 6.

¹¹⁰ OMB Memorandum M-03-22, at 6.

¹¹¹ OMB Memorandum M-03-22, at 6.

¹¹² OMB Memorandum M-03-22, at 6.

- (d) Whether the Commission is creating a new system of records or is modifying an existing system of records under the Privacy Act.¹¹³
- (E) Requests for an extension of an existing ICR do not require a new or revised PIA; however, a revised ICR may require a new or revised PIA, depending upon where the revised ICR is now adding PII or changing the PII that is part of the ICR.¹¹⁴

¹¹³ OMB Memorandum M-03-22, at 6.

¹¹⁴ OMB Memorandum M-03-22, at 6.

CHAPTER 10

COMPUTER MATCHING PROGRAM GUIDELINES

10-1. Federal Policy. The Privacy Act, the *Computer Matching and Privacy Protection Act of 1988* (“CMPPA”), and OMB regulations provide special guidelines to be followed in Federal agencies programs that conduct computer matches of the personal records in the IT information systems of two or more Federal agencies, or with a non-Federal entities.¹

- (A) The guidelines are intended to strike a balance between the efficient operation of Federal agencies and the need to protect individual privacy in the course of collecting, using, or disseminating PII.²
- (B) These guidelines do **not** authorize matching programs as such, and the Commission must justify each matching program based on its merits and in accordance with the OMB guidelines.³

10-2. Definitions. For the purposes of this directive, the following definitions shall apply:

- (A) **Data Integrity Board (DIB)** is composed of a group of senior Commission officials, including senior privacy officials, designated by the Managing Director, who are responsible, among other things, for reviewing all FCC proposals to conduct or participate in a matching program and conducting an annual review of all matching programs in which the FCC has participated.⁴ The DIB’s functions and activities are explained in detail in Chapter 11.
- (B) **Matching activity** is any computerized comparison of two or more automated sets of information about individuals. A matching activity may or may not constitute a matching program under the Privacy Act.⁵
- (C) **Matching agreement** means a written agreement between a recipient agency and a source agency (or non-Federal agency) that is required by the Privacy Act for parties engaging in a matching program.⁶
- (D) **Matching notice** means the notice published by an agency in the Federal Register upon the establishment, re-establishment, or alteration of a matching program that describes the existence and character of a matching program. A matching notice identifies the agencies involved, the purpose(s) of the matching program, the authority for conducting the matching program, the records and individuals involved, and additional details about the matching program.⁷

¹ 5 U.S.C. 552a(o)(1); Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503); OMB Circular A-130, at 8(a)(1)(i) and 8(a)(9)(c); OMB Circular A-108 (2016).

² 5 U.S.C. 552a(o)(1); OMB Circular A-130, at 8(a)(1)(i) and 8(a)(9)(c).

³ “Computer Matching and Privacy Protection Act of 1988,” Pub. L. 100-503.

⁴ OMB Circular A-108 (2016), at 4.

⁵ OMB Circular A-108 (2016), at 4; 5 U.S.C. 552a(u)(2).

⁶ OMB Circular A-108 (2016), at 4; 5 U.S.C. 552a(o).

⁷ OMB Circular A-108 (2016), at 4; 5 U.S.C. 552a(e)(12).

- (E) **Federal benefit program** is any program administered or funded by the Federal Government, or by any agency or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.⁸
- (F) **Federal personnel** are officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).⁹
- (D) **Hit** is the identification, through a matching program, of a specific individual.¹⁰
- (E) **Matching agency** generally, is the recipient Federal agency (or the Federal source agency in a match conducted by a non-Federal agency) is the matching agency and is responsible for meeting the reporting and publication requirements associated with the matching program.¹¹

However, in large, multi-agency matching programs, where the recipient agency is merely performing the matches and the benefit accrues to the source agencies, the partners should assign responsibility for compliance with the administrative requirements in a fair and reasonable way. This may mean having the matching agency carry out these requirements for all parties, having one participant designated to do so, or having each source agency do so for its own matching program(s).¹²

- (F) **Non-Federal agency** is any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program.¹³
- (G) **Personal record (i.e., PII)**, also known as a **record**, is any item, collection, or grouping of information about an individual that is maintained by the Commission, including, but not limited to, his/her education, financial transactions, medical history, and criminal or employment history and that contains his/her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.¹⁴
- (H) **Recipient Agency** means the Commission or other Federal agency or their contractors, which receives records contained in a system of records from a source agency for use in a matching program.¹⁵

⁸ 5 U.S.C. 552a(a)(12).

⁹ 5 U.S.C. 552a(a)(13).

¹⁰ FCC Privacy Act Manual (12/13/1995), at Section 9-1(c).

¹¹ OMB Circular A-130, Appendix I, at 2(b).

¹² OMB Circular A-130, Appendix I, at 2(b).

¹³ 5 U.S.C. 552a(a)(10); OMB Circular A-130, Appendix I, at 2(c).

¹⁴ 5 U.S.C. 552a(a)(4); 47 CFR § 0.551(b)(2).

¹⁵ 5 U.S.C. 552a(a)(9); OMB Circular A-130, Appendix I, at 2(d).

(I) **Recipient (Records)** are those records that are contained in a system of records from a source agency for use in a matching program.¹⁶

(J) **Source agency** is the Federal agency, which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program.¹⁷

Note: In some circumstances, a source agency may be the instigator and ultimate beneficiary of the matching program, as when an agency lacking computer resources uses another agency to perform the match.¹⁸

10-3. **Matching Programs** A **matching program** is a procedure in which a computer is used to compare two or more automated systems of records in an IT information system(s) or database containing PII, or a system of records with a set of non-Federal records to find individuals who are in common to more than one information system or database set.¹⁹

(A) The matching program consists of all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the “hits,” and disposition of the PII or records maintained in connection with the match.²⁰

(B) It should be noted that a single matching program may involve several matches among a number of participants.²¹

(C) The matching program’s objectives include:

(1) Establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance, or payments under Federal benefit programs,²² or

(2) Recouping payments or delinquent debts under Federal benefit programs.²³

(E) Matching programs do not include:

(1) Matches done to produce aggregate statistical data without personal identifiers, *i.e.*, PII or records.²⁴

¹⁶ 5 U.S.C. 552a(a)(9).

¹⁷ 5 U.S.C. 552a(a)(11); OMB Circular A-130, Appendix I, at 2(e).

¹⁸ OMB Circular A-130, Appendix I, at 2(b).

¹⁹ 5 U.S.C. 552a(a)(8)(A); OMB Circular A-108 (2016), at 4.

²⁰ 5 U.S.C. 552a(a)(8)(A).

²¹ 5 U.S.C. 552a(a)(8)(A)(i).

²² 5 U.S.C. 552a(a)(8)(A)(i)(I).

²³ 5 U.S.C. 552a(a)(8)(A)(i)(II).

²⁴ 5 U.S.C. 552a(a)(8)(B)(i).

- (2) Matches done to support any research or statistical project when the specific data are not used to make decisions about the specific individual's rights, benefits, or privileges.²⁵
- (3) Matches performed by a Federal or non-Federal law criminal enforcement agency or one of its components during the course of a criminal or civil law enforcement investigation to gather evidence against a specific person or persons.²⁶
- (4) Matches of tax information:
 - (a) Pursuant to the *Internal Revenue Code of 1986*;²⁷
 - (b) For tax administration as defined by the *Internal Revenue Code of 1986*;²⁸
 - (c) To intercept a tax refund due an individual pursuant to the *Social Security Act*;²⁹ or
 - (d) To intercept a tax refund due under any other tax refund intercept program authorized by statute containing notification, verification, and hearing requirements that OMB considers to be similar to the procedures in the *Social Security Act*.³⁰
- (5) Matches of Federal personnel records that are performed:
 - (a) By a Federal agency using records related to Federal personnel for routine administrative purposes, subject to OMB guidance,³¹ or
 - (b) By a Federal agency using its own records from a system of records maintained by the agency,³²

If the purpose of the matching activity is not to take any adverse financial, personal, disciplinary, or other adverse action against Federal personnel.³³
- (1) Matches to gather information for foreign counterintelligence purposes or to produce background checks for security clearance of Federal personnel or Federal contractor personnel.³⁴

²⁵ 5 U.S.C. 552a(a)(8)(B)(ii).

²⁶ 5 U.S.C. 552a(a)(8)(B)(iii).

²⁷ 5 U.S.C. 552a(a)(8)(B)(iv)(I).

²⁸ 5 U.S.C. 552a(a)(8)(B)(iv)(II).

²⁹ 5 U.S.C. 552a(a)(8)(B)(iv)(III).

³⁰ 5 U.S.C. 552a(a)(8)(B)(iv)(IV).

³¹ 5 U.S.C. 552a(a)(8)(B)(v)(I).

³² 5 U.S.C. 552a(a)(8)(B)(v)(II).

³³ 5 U.S.C. 552a(a)(8)(B)(v)(II).

³⁴ 5 U.S.C. 552a(a)(8)(B)(vi).

- (7) Matches performed pursuant to a levy authorized by the *Internal Revenue Code of 1986*.³⁵
- (8) Matches performed pursuant to the *Social Security Act* under 42 U.S.C. 402(x)(3) and 1382(e)(1).³⁶

³⁵ 5 U.S.C. 552a(a)(8)(B)(vii).

³⁶ 5 U.S.C. 552a(a)(8)(B)(viii).

CHAPTER 11

DATA INTEGRITY BOARD

- 11-1. Policy. The *Computer Matching and Privacy Protection Act of 1988*, 5 U.S.C. 552a (“CMPPA”), as amended by Section 2(b)(1) of the *Privacy Act of 1974*, requires the head of each Federal agency that may participate in any computer matching programs to establish a **Data Integrity Board (DIB)** to oversee and coordinate all matching programs, activities, and similar data sharing arrangements.¹
- 11-2. Data Integrity Board. The Data Integrity Board (DIB) is comprised of senior officials within the Commission.¹
- (A) The DIB evaluates and approves any request(s) to engage in computer matching program(s) and similar data sharing arrangements.¹
 - (B) The DIB also acts as an advisory board for the Commission for:
 - (1) Matters related to the Data Quality Act implementation and the collection and utilization of data in the performance reporting systems;² and
 - (2) The collection and utilization of data in the agency’s performance reporting systems.³
- 11-3. Membership and Responsibilities. On behalf of the FCC Chairman, the Managing Director appoints the members of the DIB.
- (A) Data Integrity Board Members include:
 - (1) The SAOP, as DIB Chairman;
 - (2) Inspector General, as *ex officio* (non-voting);
 - (3) Deputy Managing Director;
 - (4) Chief Financial Officer (CFO) or his/her representative;
 - (5) Chief of Human Capital Officer (CHO) or his/her representative;
 - (6) A representative from each B/O that engages in any matching activities and related actions. (DIB meetings are open to all B/Os.)
 - (7) Chief Information Officer (CIO) or his/her representative;
 - (8) Chief Data Officer (CDO) or his/her representative;

¹ 5 U.S.C. 552a(a)(u)(1)-(2); Computer Matching and Privacy Protection Act of 1988 (Pub. L. 100-503.

² 5 U.S.C. 552a(a)(u)(1).

³ 5 U.S.C. 552a(a)(u)(1).

- (9) Chief Information Security Officer (CISO) or his/her representative;
 - (10) General Counsel or the Privacy Legal Advisor(s); and
 - (11) Privacy Manger (DIB Secretary).
- (B) The **Board Chairman** has responsibility for oversight and coordination among the various components of the Commission. The Board Chairman shall:
- (1) Schedule and convene meetings of the Board, as necessary;
 - (2) Preside over all meetings of the Board;
 - (3) Survey all matching activities and identify those that may be subject to the CMPPA;⁴
 - (4) Notify the Office of Management and Budget (OMB) of any appeals to proposed matching agreements;⁵ and
 - (5) Notify the FCC Chairman and Congress if a matching program has been disapproved.⁶
- (C) The **Inspector General** will:
- (1) Not serve as DIB Chairman, in accordance with the Privacy Act;
 - (2) Notify OMB of any appeals to proposed matching agreements; and
 - (3) Notify the Chairman of the FCC and Congress if a matching program has been disapproved.
- (D) The **Chief Financial Officer** will serve as the DIB expert in matters concerning proposed matches of payroll and other financial records, such as recouping payments or delinquent debts under such Federal benefit programs;
- (E) The **Chief Human Capital Officer** will serve as DIB expert in matters concerning proposed matches of personnel records, such as establishing or verifying initial or continuing eligibility for Federal benefit programs;
- (F) **Privacy Manager** will serve as DIB secretary;
- (G) **Privacy Legal Advisor(s)** will provide guidance on all privacy issues as they relate to these matching activities and related actions;

⁴ FISMA requires that SAOP take a substantive role in all Commission privacy programs and policies.

⁵ FISMA requires that SAOP take a substantive role in all Commission privacy programs and policies.

⁶ FISMA requires that SAOP take a substantive role in all Commission privacy programs and policies.

- (H) Other members of the DIB shall serve as experts in matters concerning data matching, data quality, data security, and data collection and utilization (*e.g.*, IT functions), etc.⁷ Additionally they shall ensure that the B/O they represent comply with the Commission's responsibilities under the Data Quality Act's guidelines.⁸

11-4. Data Integrity Board's Duties. The DIB members will:

- (A) Review, approve, and maintain all written agreements for receipt or disclosure of Commission records for matching programs to ensure compliance with 5 U.S.C. 552a(o) of the Privacy Act, and all relevant statutes, regulations, and guidelines;⁹
- (B) Review all matching programs in which the Commission has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;¹⁰
- (C) Review all recurring matching programs in which the Commission has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;¹¹
- (D) Compile an **annual report**, which shall be submitted to the Chairman of the FCC and OMB and made available to the public on request describing the matching activities of the agency, including:¹²
 - (1) Matching programs in which the Commission has participated as a source agency or recipient agency;¹³
 - (2) Matching agreements proposed under 5 U.S.C. 552a(o) that were disapproved by the Data Integrity Board;¹⁴
 - (3) Any changes in membership or structure of the Board in the preceding year;¹⁵
 - (4) The reasons for any waiver of the requirement in 5 U.S.C. 552a(u)(4) for completion and submission of a cost-benefit analysis prior to the approval of a matching program;¹⁶
 - (5) Any violations of matching agreements that have been alleged or identified and any corrective action taken;¹⁷ and

⁷ 5 U.S.C. 552a(o)(1)(G).

⁸ *Data Quality Act*; 5 U.S.C. 552a(o)(1)(G).

⁹ 5 U.S.C. 552a(u)(3)(A).

¹⁰ 5 U.S.C. 552a(u)(3)(B).

¹¹ 5 U.S.C. 552a(u)(3)(C).

¹² 5 U.S.C. 552a(u)(3)(D).

¹³ 5 U.S.C. 552a(u)(3)(D)(i).

¹⁴ 5 U.S.C. 552a(u)(3)(D)(ii).

¹⁵ 5 U.S.C. 552a(u)(3)(D)(iii).

¹⁶ 5 U.S.C. 552a(u)(3)(D)(iv).

¹⁷ 5 U.S.C. 552a(u)(3)(D)(v).

- (6) Any other information required by the Director of OMB to be included in such report.¹⁸
- (E) Serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;¹⁹
- (F) Provide interpretation and guidance to the Commission's B/Os and staff on the requirements of 5 U.S.C. 552a(u) for matching programs;²⁰
- (G) Review Commission record keeping and disposal policies and practices for matching programs to assure compliance with 5 U.S.C. 552a (u);²¹
- (H) May review and report on any Commission matching activities that are not matching programs;²² and
- (I) Act as an "advisory board" for the Commission on matters related to the Commission's *Data Quality Act* implementation and the collection and utilization of data in the agency's performance reporting systems.²³

11-5. Cost-Benefit Analysis.

- (A) Except as provided in paragraphs (B) and (C) below, as noted in 5 U.S.C. 552a(u)(4)(B) and 552a(u)(4)(C) of the Act, the Data Integrity Board shall not approve any written agreement for a matching program unless the Commission has completed and submitted to the Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.²⁴
- (B) The Data Integrity Board may waive the requirement for a cost-benefit analysis, in paragraph (A) above, 5 U.S.C. 552a(u)(4)(A), if it determines in writing, in accordance with guidelines prescribed by the Director of OMB, that a cost-benefit analysis is not required.²⁵
- (C) A cost-benefit analysis shall not be required by paragraph (A) above, under 5 U.S.C. 552a(u)(4)(A) of the Privacy Act, prior to the initial approval of a written agreement for a matching program that is specifically required by statute.²⁶

Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the Commission has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.²⁷

¹⁸ 5 U.S.C. 552a(u)(3)(D)(vi).

¹⁹ 5 U.S.C. 552a(u)(3)(E).

²⁰ 5 U.S.C. 552a(u)(3)(F).

²¹ 5 U.S.C. 552a(u)(3)(G).

²² 5 U.S.C. 552a(u)(3)(H).

²³ 5 U.S.C. 552a(o)(1)(G).

²⁴ 5 U.S.C. 552a(u)(4)(A).

²⁵ 5 U.S.C. 552a(u)(4)(B).

²⁶ 5 U.S.C. 552a(u)(4)(C).

²⁷ 5 U.S.C. 552a(u)(4)(C).

11-6. Matching Agreement Disapproval and Right of Appeal:

- (A) If a matching agreement is disapproved by the Data Integrity Board, any party to such agreement may **appeal** the disapproval to the Director of OMB.²⁸ An appeal should be forwarded to the Director, OMB, Washington, D.C. 20503 within **30 days** following the Board's written approval.²⁹
- (1) The following documentation should accompany the appeal:
- (a) Copies of all documentation accompanying the initial matching agreement proposal;³⁰
 - (b) A copy of the Board's disapproval and reasons therefore;³¹
 - (c) Evidence supporting the cost-effectiveness of the match;³² and
 - (d) Any other information relevant to a decision, *e.g.*, timing considerations, the public interest served by the match, etc.³³
- (2) Timely notice of the filing of such an appeal shall be provided by the Director of OMB to the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committee on Oversight and Government Reform.³⁴
- (B) The Director of OMB may approve a matching agreement notwithstanding the disapproval of the Commission's Data Integrity Board if the Director determines that:³⁵
- (1) The matching program will be consistent with all applicable legal, regulatory, and policy requirements;³⁶
 - (2) There is adequate evidence that the matching agreement will be cost-effective;³⁷ and
 - (3) The matching program is in the public interest;³⁸
- (C) The decision of the Director of OMB to approve a matching agreement shall not take effect until **30 days** after it is reported to the Senate and House committees, which the

²⁸ 5 U.S.C. 552a(u)(5)(A).

²⁹ 5 U.S.C. 552a(u)(5)(A).

³⁰ 5 U.S.C. 552a(u)(5)(A).

³¹ 5 U.S.C. 552a(u)(5)(A).

³² 5 U.S.C. 552a(u)(5)(A).

³³ 5 U.S.C. 552a(u)(5)(A).

³⁴ 5 U.S.C. 552a(u)(5)(A); OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 20.

³⁵ 5 U.S.C. 552a(u)(5)(B).

³⁶ 5 U.S.C. 552a(u)(5)(B)(i).

³⁷ 5 U.S.C. 552a(u)(5)(B)(ii).

³⁸ 5 U.S.C. 552a(u)(5)(B)(iii).

Privacy Act requires under 5 U.S.C. 552a(u)(5)(A), and as noted in paragraph (A) above.³⁹

- (D) If the Data Integrity Board and the Director of OMB disapprove a matching program proposed by the Inspector General of the FCC, the Inspector General may report the disapproval to the Chairman of the FCC and to the Congress.⁴⁰

11-7. Disclosing PII for Matching Programs.

- (A) **To Another Federal Agency** – Each B/O is responsible for determining whether or not to disclose PII (*i.e.*, records) from their systems and for making sure they meet the Privacy Act’s necessary disclosure provisions when they do:⁴¹
 - (1) If the B/O is satisfied that disclosure of the records would not violate its responsibilities under the Privacy Act, then proceed to make the disclosure to the matching agency.⁴²
 - (2) Ensure that only the minimum information necessary to conduct the match is provided.⁴³
 - (3) If disclosure is to be made pursuant to a routine use, ensure that the system of records contains such a use;⁴⁴ otherwise, the B/O must publish a routine use notice in the *Federal Register*.⁴⁵
 - (4) The B/O should also be sure to maintain an accounting of the disclosures as required under 5 U.S.C. 552a(c) of the Act.⁴⁶
- (B) **To a Non-federal Entity** – Before disclosing records to a nonfederal entity matching program to be carried out by that entity, each B/O should, in addition to all of the considerations above, also make reasonable efforts, pursuant to 5 U.S.C. 552a(e)(6) of the Act, that such records are “accurate, complete, timely, and relevant for agency purposes.”⁴⁷
- (C) Before disclosing records to either a federal or nonfederal entity, each B/O should notify the SAOP, Privacy Manager, and the OGC Privacy Legal Advisor(s), who can assist with the various administrative and legal issues that are involved:⁴⁸
 - (1) Review and approval by the Data Integrity Board;⁴⁹

³⁹ 5 U.S.C. 552a(e)(12) and 552a(u)(5)(C).

⁴⁰ 5 U.S.C. 552a(u)(5)(D).

⁴¹ 5 U.S.C. 552a(o) and 552a(q).

⁴² 5 U.S.C. 552a(o)(1)(G), 552a(o)(1)(H), and 552a(q).

⁴³ 5 U.S.C. 552a(o)(1)(G).

⁴⁴ 5 U.S.C. 552a(b) and 552a(o)(1)(G),

⁴⁵ OMB Circular A-130, Appendix I, at 4(c)(1)(f), 5, and 552(a)(2)(b).

⁴⁶ 5 U.S.C. 552a(c).

⁴⁷ 5 U.S.C. 552a(e)(6), 552a(o)(1)(J), and 55a(q).

⁴⁸ OMB Circular A-130, Appendix I, at 4-5.

⁴⁹ OMB Circular A-130, Appendix I, at 4-5.

- (2) Creation of any new or revision to any existing system(s) of records, as required;⁵⁰ and
- (3) Compliance with OMB's notice and public comment requirements under the Privacy Act.⁵¹

11-8. Matching Agreement Notice. The Privacy Act requires that no record which is contained in a FCC system of records may be disclosed to a recipient Federal agency or to a non-Federal agency for use in a computer matching program except pursuant to a **written agreement** between the source agency (*i.e.*, the Commission) and the recipient Federal agency or non-Federal agency specifying.⁵²

- (A) For this agreement to go into effect, the recipient agency (or source agency where the recipient is a non-Federal agency) must publish a notice in the *Federal Register* describing this established, re-established, or altered matching program agreement.⁵³
- (B) The matching notice should appear in the format prescribed by *the Office of the Federal Register's Document Drafting Handbook* as shown in Appendix 2.⁵⁴
- (C) A matching agreement notice should contain the following elements:⁵⁵
 - (1) A **heading** identifying the document as a matching notice, an **agency** line naming the specific agency that is publishing the notice, and an **action** line indicating whether the notice describes a "new" or "altered" matching program. The purpose and legal authority for conducting the matching program;⁵⁶
 - (2) The name of the **participating agency or agencies** (including any non-Federal agencies);⁵⁷
 - (3) The **beginning and ending dates** of the matching program, including a note about the possibility of a one-year renewal of by the Data Integrity Board;⁵⁸
 - (4) A **plain-language description** of the matching program and its purpose(s) and/or justification(s);⁵⁹
 - (5) The **specific authority(s)** for conducting the matching program;⁶⁰

⁵⁰ OMB Circular A-130, Appendix I, at 4-5.

⁵¹ OMB Circular A-130, Appendix I, at 4-5.

⁵² 5 U.S.C. 552a(o)(1).

⁵³ OMB Circular A-108 (2016), at 19; 5 U.S.C. 552a(o).

⁵⁴ OMB Circular A-108 (2016), 19; 5 U.S.C. 552a(o); NARA, *Document Drafting Handbook*, at 3-23.

⁵⁵ OMB Circular A-108 (2016), 19; 5 U.S.C. 552a(o); NARA, *Document Drafting Handbook*, at 3-23.

⁵⁶ OMB Circular A-108 (2016), at 19; 5 U.S.C. 552a(o).

⁵⁷ OMB Circular A-108 (2016), at 19; 5 U.S.C. 552a(o).

⁵⁸ OMB Circular A-108 (2016), at 19; 5 U.S.C. 552a(o).

⁵⁹ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1)(B).

⁶⁰ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1)(A).

- (6) The **categories of records** that will be matched, *i.e.*, description of the information or data elements that will be used and the approximate number of records that will be matched;⁶¹
- (7) The **categories of individuals** whose information is involved in the matching program;⁶²
- (8) The names of the relevant **system(s) of records** and a citation of the SORNs;⁶³
- (9) The name, title, business address, and **contact information** of the agency official who is responsible for the matching program;⁶⁴
- (10) Instructions for **submitting comments** on the matching program, including an e-mail address or a website where comments can be submitted electronically;⁶⁵ and
- (11) A **supplementary information** section that provides any other relevant information about the matching program.⁶⁶

11-9. Publication Requirements.

- (A) Under 5 U.S.C. 552a(o)(2) and 552a(r) Privacy Act and OMB guidelines, each agency that proposes to **establish, re-establish, or significantly alter** a matching program must publish a notice in the *Federal Register* and notify OMB and the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committee on Oversight and Government Reform of any such matching activities. The agency publication and notification requirements pertain to:⁶⁷
 - (1) The **recipient Federal agency** or the **Federal source agency** in a match conducted by a **non-Federal agency**;⁶⁸ or
 - (2) When the recipient agency is **not** the actual beneficiary of the matching program, it may to the extent legally permissible, negotiate with the actual

⁶¹ 5 U.S.C. 552a(o)(1)(C).

⁶² OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1)(C).

⁶³ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1)(C).

⁶⁴ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1).

⁶⁵ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1)(D).

⁶⁶ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 19; 5 U.S.C. 552a(o)(1)(D).

⁶⁷ OMB Circular A-108 (2016), at 20; 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2), and 552a(r).

⁶⁸ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 20; 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2), and 552a(r).

beneficiary agency for reimbursement of the costs incurred in publishing the matching program notice.⁶⁹

- (3) The **re-establishment** of a matching program, which is when an agency re-establishes a matching program upon the expiration of a matching agreement. As with new or altered matching agreements, the re-establishment of a matching program requires the publication of a matching notice in the *Federal Register* and needs to be reported to OMB and Congress.⁷⁰
- (4) The **renewal** of a matching program, which occurs when the agency's DIB renews a matching agreement for one additional year pursuant to 5 U.S.C. 552a(o)(2)(D).⁷¹

Note: The matching program's renewal does **not** require the publication of a matching notice and does not need to be reported to OMB and Congress.⁷²

- (B) The criteria for the publication and notification requirements include one or more the following circumstances:⁷³
 - (1) Before disclosing records outside the Commission under a new routine use pursuant to a matching agreement, as required by 5 U.S.C. 552a(b)(3) and 552a(e)(11) of the Act.⁷⁴
 - (2) If the matching program will result in the creation of a new or the substantial alteration of an existing system of records, under 5 U.S.C. 552a(o) and 552a(r) of the Act.⁷⁵
 - (3) When the Commission proposes to carry out a new or substantially altered matching program, under 5 U.S.C. 552a(o)(2) and 552a(r) of the Act.⁷⁶
 - (a) A "minor change to a matching program" is one that does **not** significantly alter the terms of the agreement under which the program is being carried out.⁷⁷

⁶⁹ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 20; 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2), and 552a(r).

⁷⁰ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 20; 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2).

⁷¹ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 20; 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2)(D).

⁷² OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 20; 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2)(D).

⁷³ 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2), and 552a(r); OMB Circular A-108 (2016), at 20; OMB Circular A-130, Appendix I, at 4(d), 5, 5(a), and 5(b).

⁷⁴ 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2), and 552a(r); OMB Circular A-130, Appendix I, at 4(c), 4(d), 5, 5(a), and 5(b); and 47 CFR §§ 0.552 – 0.553.

⁷⁵ 5 U.S.C. 552a(o)(2), and 552a(r); and OMB Circular A-130, Appendix I, at 4(d), 5, 5(a), and 5(b)(2).

⁷⁶ 5 U.S.C. 552a(o)(2) and 552a(r); and OMB Circular A-130, Appendix I., at 4(d), 5, 5(a) – 5 (b).

⁷⁷ OMB Circular A-130, Appendix I, at 4(d)(1).

- (b) Examples of significant changes include:
 - (i) Changing the purpose for which the program was established;⁷⁸
 - (ii) Changing the matching population, either by including new categories of record subjects or by greatly increasing the numbers of records matched;⁷⁹
 - (iii) Changing the legal authority covering the matching program;⁸⁰ and
 - (iv) Changing the source or recipient agencies involved in the matching program.⁸¹

(B) The publication and public notice requirements under the Privacy Act and OMB guidelines are as follows:

- (1) Publish the notice in the *Federal Register* to describe any proposal to establish, re-establish, or substantially alter a matching program and provide at least **40 days** prior to the start of this matching program;⁸² and

Note: *Appendix 3, Office of the Federal Register Matching Activities Notice Template.*

- (2) Submit reports to OMB and the Chairman and Ranking Member of the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committee on Oversight and Government Reform to provide adequate advance notice of any such proposal in order to permit an evaluation of the probable or potential effect(s) of such proposal on the privacy or other rights of individuals.⁸³
- (3) The reports must be submitted as follows:
 - (a) At least **40 days** prior to the initiation of any matching activity carried out under a new or substantially altered matching program.⁸⁴
 - (b) For **renewals** of continuing programs, the report must be dated at least **40 days** prior to the expiration of any existing matching agreement.⁸⁵

⁷⁸ OMB Circular A-130, Appendix I, at 4(d)(1)(a).

⁷⁹ OMB Circular A-130, Appendix I, at 4(d)(1)(b).

⁸⁰ OMB Circular A-130, Appendix I, at 4(d)(1)(c).

⁸¹ OMB Circular A-130, Appendix I, at 4(d)(1)(d).

⁸² 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2), and 552a(r); OMB Circular A-108, at 21; OMB Circular A-130, Appendix I, at 4(c)-(4)d and 5 – 5(b).

⁸³ 5 U.S.C. 552a(e)(11) – 552a(e)(12), 552a(o)(2), and 552a(r); and OMB Circular A-130, Appendix I, at 4(c) – 4(d), 5, 5(a) – 5(b).

⁸⁴ 5 U.S.C. 552a(e)(12); and OMB Circular A-130, Appendix I, at 4(d).

⁸⁵ 5 U.S.C. 552a(e)(12); and OMB Circular A-130, Appendix I, at 4(d)

- (c) When re-establishing a matching program and continuing the program past the expiration of the current matching agreement (including any one-year renewal approved by the DIB), the agency shall report the proposal to re-establish the matching program at least **40 days** prior to the expiration of the existing matching agreement.⁸⁶
- (C) The Commission may ask the Director of OMB/OIRA for **expedited review** of the proposed change(s).⁸⁷ In such case:
 - (1) OMB may grant a waiver of the **40 day** review period for either systems of records or matching program reviews,⁸⁸ but
 - (2) OMB cannot waive time periods specifically established by the Privacy Act, such as the **30 day** notice and comment period required for the adoption of a routine use proposal, pursuant to 5 U.S.C. 552a(b)(3) of the Privacy Act.⁸⁹

11-10. Matching Program Report. The report for a new or altered matching program has three elements: a **Transmittal letter**, a **Narrative Statement**, and any **supporting documentation**, which includes a copy of the proposed *Federal Register* notice for the matching agreement program.⁹⁰ (The requirements for a matching report are similar to those for a new or altered SORN.)

- (A) While there is no specific form for the **Transmittal Letter**, the letter should serve as a brief cover letter accompanying the matching program report. The transmittal letter must include:⁹¹
 - (1) Signature of the SAOP (or his/her designee) or the DIB chairman;⁹²
 - (2) The name, e-mail address, and telephone number of the individual who can best answer questions about the matching program;⁹³ and
 - (3) The agency's assurance that the proposed matching program was approved by the DIB and fully complies with the Privacy Act and OMB policies;⁹⁴
 - (4) A statement that a copy of the matching agreement has been distributed to Congress as the Privacy Act requires;⁹⁵ and
 - (5) A request to OMB for waiver of the review time period under the OMB "expedited review" guidelines, when appropriate or necessary.⁹⁶

⁸⁶ OMB Circular A-108 (2016), at 21.

⁸⁷ OMB Circular A-130, Appendix I, at 4(e).

⁸⁸ OMB Circular A-130, Appendix I, at 4(e).

⁸⁹ 5 U.S.C. 552a(e)(11), 552a(e)(12), 552a(o)(2)(B); OMB Circular A-130, Appendix I, at 4(e).

⁹⁰ OMB Circular A-130, Appendix I, at 4(d).

⁹¹ OMB Circular A-130, Appendix I, at 4(d).

⁹² OMB Circular A-130, Appendix I, at 4(d).

⁹³ 5 U.S.C. 552a(b)(3); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(a).

⁹⁴ 5 U.S.C. 552a(b)(3); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(a).

⁹⁵ 5 U.S.C. 552a(b)(3); OMB Circular A-130, Appendix I, at 4(d)(2)(a).

⁹⁶ 5 U.S.C. 552a(o)(1)(D); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(a).

- (B) The **Narrative Statement** should also be brief but comprehensive and provide an overview of the proposed matching program, making reference to the information in the supporting documentation. It should also not simply restate information provided in the supporting documentation, but it should:⁹⁷
- (1) Describe the **purpose(s)** for which the agency is establishing, re-establishing, or significantly altering the matching program;⁹⁸
 - (2) Identify the **specific authority** (statute or executive order) under which the agency is conducting the matching program. The agency should avoid citing authority that is overly general; rather, the agency shall cite the specific programmatic authority for conducting the matching program);⁹⁹
 - (3) Describe the administrative, technical, and physical **security safeguards** in place to protect against any unauthorized access or disclosure of records used in the matching program;¹⁰⁰
 - (4) Provide the agency's specific evaluation of the **potential impact(s) on the privacy** of individuals whose records will be used in the matching program;¹⁰¹ and
 - (5) Indicate whether a **cost-benefit analysis** was performed for the matching program, describe the results of the cost/benefit analysis required by 5 U.S.C. 552a(u)(4)(A) of the Privacy Act, and explain the basis on which the agency is justifying the matching program.¹⁰²
- (C) The following **supporting documentation** shall be included with all reports of an established, re-established, or significantly altered matching program: ¹⁰³
- (1) A copy of the *Federal Register* matching notice (in the prescribed matching notice template) describing the matching program, as shown in Appendix 2.¹⁰⁴
 - (2) For significantly altered matching programs, the agency shall include:
 - (a) A list of the substantive changes to the previously published version of the matching notice;¹⁰⁵ and

⁹⁷ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b).

⁹⁸ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b).

⁹⁹ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(1).

¹⁰⁰ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(2).

¹⁰¹ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(3).

¹⁰² 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24-25; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(3).

¹⁰³ 5 U.S.C. 552a(r); OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1);

Document Drafting Handbook, at 3-23.

¹⁰⁴ OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1); *Document Drafting Handbook*, at 3-23

¹⁰⁵ OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1); *Document Drafting Handbook*, at 3-23

- (b) A version of the previously published matching notice that has been marked up to show the changes that are being proposed.¹⁰⁶
- (c) The full matching agreement that was approved by the agency's DIB.¹⁰⁷

11-11. Publication, Review, and Comment. The Matching Activity requirement include:

- (A) Publication of the FR matching activity notice must occur at least **30 days** prior to the initiation of any matching activity carried out under a new or substantially altered matching program to allow the public time to submit comments to OMB.¹⁰⁸
- (B) OMB guidelines request that the FCC (*i.e.*, B/O which is carrying out the matching activity) should ensure that the letters and the draft matching notice documents package should be submitted to OMB and Congress expeditiously after the transmittal letters are signed.¹⁰⁹
- (C) A copy of each new or altered matching agreement entered into, pursuant to 5 U.S.C. 552a(o)(2)(A) of the Privacy Act,¹¹⁰ and shall be sent to:
 - (1) The Chairman and Ranking Member of the H.R. and Senate committees on government oversight;¹¹¹ and
 - (2) The Administrator of the Office of Information and Regulatory Affairs (OIRA), Office of Management and Budget (OMB).¹¹²
- (D) No such matching agreement shall be effective until **40 days** after the date on which such a copy is transmitted to the Director of OMB and the House and Senate committees. The review and publication timelines should run as follows:

¹⁰⁶ 5 U.S.C. 552a(r); OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1); *Document Drafting Handbook*, at 3-23. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(1).

¹⁰⁶ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(2).

¹⁰⁶ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(3).

¹⁰⁶ 5 U.S.C. 552a(o); OMB Circular A-108 (2016), at 24-25; OMB Circular A-130, Appendix I, at 4(d)(2)(b)(3).

¹⁰⁶ 5 U.S.C. 552a(r); OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1); *Document Drafting Handbook*, at 3-23.

¹⁰⁶ OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1); *Document Drafting Handbook*, at 3-23

¹⁰⁶ OMB Circular A-108 (2016), at 25; OMB Circular A-130, Appendix I, at 4(d)(2)(c)(1); *Document Drafting Handbook*, at 3-23

¹⁰⁷ 5 U.S.C. 552a(r); OMB Circular A-108 (2016), at 25.

¹⁰⁸ OMB Circular A-130, Appendix I, at 5(b)(3)(d); 5 U.S.C. 552a (o)(2)(B).

¹⁰⁹ 5 U.S.C. 552a(o)(2)(A); OMB Circular A-130, Appendix I, at 4 (d)(4).

¹¹⁰ 5 U.S.C. 552a(o)(2) and 552a(r); OMB Circular A-130, Appendix I, at 4, 4(d), 5, and 5(b)(2).

¹¹¹ 5 U.S.C. 552a(o)(2)(A)(i) and 552a(r); OMB Circular A-130, Appendix I, at 4, 4(d), 5, and 5(b)(2).

¹¹² OMB Circular A-130, Appendix I, at 4 and 4(d).

- (1) This **40 day review period** now includes an initial, advanced **10 day review** that OMB and Congress must have prior to publication of the notice in the *Federal Register*.¹¹³
 - (2) The 10 day advanced review is then followed by the full **30 day review** period that may coincide with the Federal Register publication.¹¹⁴
 - (3) The purpose of the initial 10 day review period is to allow OMB and Congress to perform an initial review of the proposal and, if possible, to provide the agency with the opportunity to make any changes to the matching notice before publication.¹¹⁵
 - (4) The initial, advanced 10 day review period is **not** a substitute for the full 40 day review process, and OMB and Congress may provide comments at any time over the full 40 day review period.¹¹⁶
 - (5) If any agency needs to make changes to a matching notice based on comments from OMB or Congress after the notice has been published in the Federal Register, the agency will be required to publish a revised version of the notice.¹¹⁷
 - (6) Therefore, the agency may decide to wait to publish the matching notice until the end of the full 40 day review period if the agency wishes to avoid the possibility of publishing a revised version of the matching notice.¹¹⁸
- (E) Following the 10 day advanced review and OMB (and Congressional) approval of the draft, the FCC will then publish the matching program public notice in the *Federal Register*.
- (1) Once the FR notice is published, it and the other matching activity documents should be available upon request to the public.¹¹⁹

¹¹³ OMB Circular A-108 (2016), at 21; 5 U.S.C. 552a(o)(2)(B); OMB Circular A-130, Appendix I, at 4(d) and 5(b)(2).

¹¹⁴ OMB Circular A-108 (2016), at 21; 5 U.S.C. 552a(o)(2)(B); OMB Circular A-130, Appendix I, at 4(d) and 5(b)(2).

¹¹⁵ OMB Circular A-108 (2016), at 21; 5 U.S.C. 552a(o)(2)(B); OMB Circular A-130, Appendix I, at 4(d) and 5(b)(2).

¹¹⁶ OMB Circular A-108 (2016), at 21; 5 U.S.C. 552a(o)(2)(B); OMB Circular A-130, Appendix I, at 4(d) and 5(b)(2).

¹¹⁷ 5 U.S.C. 552a(o)(2)(A)(ii) and 552a(r); OMB Circular A-108 (2016), at 16; OMB Circular A-130, Appendix I, at 4 and 4(d).

¹¹⁸ 5 U.S.C. 552a(o)(2)(A)(ii) and 552a(r); OMB Circular A-108 (2016), at 16; OMB Circular A-130, Appendix I, at 4 and 4(d).

¹¹⁹ 5 U.S.C. 552a(o)(2)(A)(ii) and 552a(r); OMB Circular A-108 (2016), at 16; OMB Circular A-130, Appendix I, at 4 and 4(d).

- (2) Upon publication the formal 40 day review period for OMB and Congress begins, while the public has the first 30 days of this formal review period in which to submit comments to OMB.¹²⁰
- (3) These two review periods run **concurrently**, but OMB and Congress have the final 10 day days of this time to review any public comments that are submitted.¹²¹
- (4) Approximately a week to **10 business days** before the expiration of the **40 day review period** the Privacy Manager also should contact OMB to ascertain whether OMB will provide comments on the proposed matching activity.¹²²
- (F) The matching agreement may remain in effect for a maximum of **30 months: 18 months** from the date that the matching agreement goes into effect (“the initial eligibility”) plus an extension of up to **12 months**.¹²³
- (H) It is up to the Commission’s Data Integrity Board to determine the length of the matching agreement, based on the purpose(s) and length of time necessary to conduct the matching program.¹²⁴

11-12. Renewals of Matching Programs.

- (A) Within **3 months** prior to the **expiration** of a matching agreement, pursuant to 5 U.S.C. 552a(o)(2)(C), the DIB may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if:¹²⁵
 - (7) The matching program will be conducted without any change;¹²⁶ and
 - (2) Each party to the matching agreement certifies to the Data Integrity Board in writing that the program has been conducted in compliance with the agreement.¹²⁷
- (B) If agencies wish to continue a matching program past the **30 month** period of initial eligibility (*i.e.*, the initial **18 months** plus a **one year** extension), the Privacy Act and OMB guidelines require the Federal agency(s) in the matching program to submit a report to OMB and Congress and publish a public notice in the *Federal Register*.¹²⁸
- (C) The report should include the following:

¹²⁰ OMB Circular A-108 (2016), at 16; 5 U.S.C. 552a(o)(2); OMB Circular A-130, Appendix I, at 4(d)(4).

¹²¹ OMB Circular A-108 (2016), at 16; 5 U.S.C. 552a(o)(2); OMB Circular A-130, Appendix I, at 4(d)(4).

¹²² OMB Circular A-130, Appendix I, at 4(d)(4).

¹²³ 5 U.S.C. 552a(o)(2)(C); OMB Circular A-130, Appendix I, at 5(b)(2).

¹²⁴ 5 U.S.C. 552a(o)(2)(C); OMB Circular A-130, Appendix I, at 5(b)(2).

¹²⁵ 5 U.S.C. 552a(o)(2)(D); OMB Circular A-130, Appendix I, at 5(b)(2).

¹²⁶ 5 U.S.C. 552a(o)(2)(D)(i).

¹²⁷ 5 U.S.C. 552a(o)(2)(D)(ii).

¹²⁸ 5 U.S.C. 552a(o)(2)(D) and 552a(r); OMB Circular A-130, Appendix I, at 5(b)(2).

- (1) All of the components of the initial matching report, *i.e.*, the Transmittal Letter, Narrative Statement, and the supporting documentation as prescribed by the Federal Register's *Document Drafting Handbook*;
 - (2) The *Federal Register* notice
 - (3) A copy of the matching agreement (for the two Congressional committees only) as outlined above;¹²⁹
- (D) The timeline for getting renewal of the matching program approved is:
- (1) The report to OMB and the Senate Committee on Homeland Security and Governmental Affairs and the H.R. Committee on Oversight and Government Reform requesting renewal of the matching program must be dated at least **40 days prior** to the expiration of the existing matching agreement following the timeline stated above;¹³⁰
 - (2) The public notice in *Federal Register* for this renewal must be published at least **40 days prior** to the expiration of the existing matching agreement;¹³¹ however,
 - (3) The Commission may request **expedited review** for the matching agreement, which reduces the public comment period from 40 to 30 days, as explained below.¹³²
- (E) If **renewal** of the matching program results in the creation of a new or the substantial alteration of an existing system of records, the Privacy Manager will work with the B/O, which is responsible for operating the system(s) of records, to follow the review, comment, and publication timeline:¹³³
- (1) Submit the draft SORN and accompanying documents (*i.e.*, transmittal letter, narrative statement and supplementary documents) to OMB and the two Congressional committees for the **10-day advanced review** and comments, if any;¹³⁴ and
 - (2) Upon the initial clearance by OMB and Congress, then publish the SORN in the *Federal Register* for the new or altered system of records, consistent with 5 U.S.C. 552a(e)(4)(D) of the Privacy Act. This begins the **40 day** public comment period, unless an **expedited review** waiver (30 day review period) is granted.¹³⁵ and

¹²⁹ 5 U.S.C. 552a(o)(2) and 552a(r); OMB Circular A-130, Appendix I, at 4(d)(2)(a) and 5(b)(2).

¹³⁰ 5 U.S.C. 552a(o)(2)(A) and 552a(r); OMB Circular A-130, Appendix I, at 4(d) and 5(b)(2).

¹³¹ OMB Circular A-130, Appendix I, at 5(b)(2); 5 U.S.C. 552a(o)(2)(B).

¹³² OMB Circular A-130, Appendix I, at 4(e).

¹³³ 5 U.S.C. 552a(e)(4) and 552a(e)(11); 47 CFR § 0.552; OMB Circular A-130, Appendix I, at 4(c) and 5(a)(1).

¹³⁴ 5 U.S.C. 552a(e)(4) and 552a(e)(11); 47 CFR § 0.552; OMB Circular A-108 (2016), at 13; OMB Circular A-130, Appendix I, at 4(c) and 5(a)(1).

¹³⁵ OMB Circular A-108 (2016), at 15-16; U.S.C. 552a(e)(4) and 552a(e)(11); 47 CFR § 0.552; OMB Circular A-130, Appendix I, at 4(c) and 5(a)(1).

- (F) The B/O and the Privacy Manager will work together to ensure that:
- (1) The SORN package (for this new or substantially altered system of records) is submitted to OMB and Congress for their initial advanced 10 day review and comment period, noted above;¹³⁶ and
 - (2) The SORN (incorporating any OMB and/or Congressional comments) is subsequently published in the Federal Register for the 40 day public comment period, far enough in advance to meet OMB guidelines for approval of the system of records **prior** to expiration of the current matching agreement.¹³⁷
- (G) Unless OMB grants a waiver under **expedited review**, as noted below, such approval requires submission of these documents more than 40 days in advanced of the matching agreement's expiration to meet the **40 day review** by OMB and Congressional, including the **30 day** public notice and comment period following publication of the SORN in the *Federal Register*.¹³⁸
- (H) The SORN package (for this new or substantially altered system of records) is submitted to OMB and Congress for their initial advanced 10 day review and comment period, noted above, and that the SORN is subsequently published in the Federal Register for the 40 day public comment period, far enough in advance to meet OMB guidelines for approval of the system of records **prior** to expiration of the current matching

11-13. Expedited Review. The Director of OMB may grant a waiver of the **40 day** review period for either the SORN or the matching program reviews under **expedited review**.¹³⁹

- (A) The B/O and the Privacy Manager should notify the OMB desk officer as soon as possible that the Commission is seeking expedited review for the matching program and/or the related SORN.

Note: Generally, the OMB desk officer will request that the Commission conduct a conference call and/or prepare an explanatory e-mail stating the reasons for this expedited review waiver and the necessary justification for this waiver.

- (B) The **Transmittal Letter** to OMB, as noted above) includes the request for the waiver and should reiterate the reasons that were stated in the conference call or e-mails for the expedited review waiver in **its transmittal letter** to OMB and demonstrate compelling reasons. When a waiver is granted, the Commission is not thereby relieved of any other requirement of the Privacy Act, as explained above.¹⁴⁰

¹³⁶ 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2)(A) – (o)(2)(B), and 552a(r); OMB Circular A-130, Appendix I, at 4(c), 4(d), 5, 5(a), and 5(b).

¹³⁷ 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2)(A) – (o)(2)(B), and 552a(r); OMB Circular A-130, Appendix I, at 4(c), 4(d), 5, 5(a), and 5(b).

¹³⁸ 5 U.S.C. 552a(e)(4), 552a(e)(11), 552a(o)(2)(A) – (o)(2)(B), and 552a(r); OMB Circular A-130, Appendix I, at 4(c), 4(d), 5, 5(a), and 5(b).

¹³⁹ OMB Circular A-130, Appendix I, at 4(e).

¹⁴⁰ OMB Circular A-130, Appendix I, at 4(e).

- (C) If **no** waiver is granted, the privacy manager will contact the OMB desk officer several days before the expiration of the **40 day review period** to inquire if OMB intends to comment on the matching system and/or SORN.¹⁴¹
- (D) OMB **cannot** waive the time periods specifically established by the Privacy Act, such as the **30 day** notice and comment period required for the adoption of a routine use proposal, pursuant to 5 U.S.C. 552a(b)(3) of the Privacy Act.¹⁴²

11-14. Annual B/O Matching Activities Reviews. As required by the *Computer Matching and Privacy Protection Act of 1988* (Public Law (Pub. L.) 100-503) (“CMPPA”), and as part of the annual FISMA review, the SAOP has instructed the Privacy Manager to conduct a review with representatives of each B/O to discuss any data matching activities and/or data sharing arrangements in which their B/O may have been engaged during the fiscal year.¹⁴³

- (A) The results of each B/O interview are compiled in a **Matching Activities Checklist** (“Checklists”), which the B/O representatives and the Privacy Manager both sign;¹⁴⁴

Note: *Appendix 4, Matching Activities Checklist.*

- (B) The Checklists are submitted to the SAOP for his review and sign-off;
- (C) The OGC Privacy Legal Advisors also review these checklists and a follow-up meeting may be held, depending upon the results of these annual B/O interviews and their findings.
- (D) This meeting provides an opportunity for the OGC Legal Advisors to explore any legal issues and related concerns that they may have with the B/O representatives, Privacy Manager, and the SAOP concerning these data sharing arrangements and/or matching activities.
- (C) The Privacy Manager and the B/Os each retain a copy of their checklist. The checklist files must also be available for review by OMB, GAO, the Comptroller General, and other Federal entities to insure that proper safeguards are being used to protect personal data and to oversee agency management of computer match decision-making.¹⁴⁵
- (D) The findings of these annual B/O reviews is the basis for:
 - (1) The Commission’s annual Data Integrity Board meeting, chaired by the SAOP;¹⁴⁶

¹⁴¹ OMB Circular A-130, Appendix I, at 4(e).

¹⁴² 5 U.S.C. 552a(b)(3); OMB Circular A-130, Appendix I, at 4(e) and 5(a)(2)(b).

¹⁴³ 5 U.S.C. 552a(o).

¹⁴⁴ 5 U.S.C. 552a(o).

¹⁴⁵ 5 U.S.C. 552a(c), 552a(o)(1)(D), 552a(o)(1)(G), and 552a(o)(1)(K); OMB Circular A-130, Appendix I, at 4(d).

¹⁴⁶ 5 U.S.C. 552a(o) and 552a(s); OMB Circular A-108, OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30; OMB Circular A-130, Appendix I, at 4(b).

- (2) The Commission's Annual Matching Activity Review and Report to OMB;¹⁴⁷
- (3) Responses to several questions in SAOP privacy report that is part of the Commission's annual FISMA submission to OMB and Congress.¹⁴⁸
- (E) This file must also be available for review by OMB, GAO, the Comptroller General, and other Federal entities to insure that proper safeguards are being used to protect personal data and to oversee agency management of computer match decision-making.¹⁴⁹

11-15. Contractors.

- (A) Matching programs should, as far as practicable, be conducted "in-house" by Federal agencies using agency personnel, rather than by contractors.¹⁵⁰
- (A) When the Commission (or other Federal agency) provides by contract for the operation by, or on behalf of the agency, of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of 5 U.S.C. 552a(m) to be applied to the system of records.¹⁵¹
- (B) Pursuant to 5 U.S.C. 552a(i), any contractor and any employee of the contractor (if the contract is agreed to on or after 1974) shall be considered to be an employee of the Commission;¹⁵² and therefore:
 - (1) The terms of the contract should include appropriate privacy and security provisions consistent with policies, regulations, standards, and guidelines issued by OMB, General Services Administration (GSA), and the Department of Commerce;¹⁵³
 - (2) The terms of the contract should preclude the contractor from using, disclosing, copying, or retaining records associated with the matching program for the contractor's own use;¹⁵⁴

¹⁴⁷ 5 U.S.C. 552a(o) and 552a(s); OMB Circular A-108, OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30; OMB Circular A-130, Appendix I, at 4(b).

¹⁴⁸ 5 U.S.C. 552a(o) and 552a(s); OMB Circular A-108, OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30; OMB Circular A-130, Appendix I, at 4(b).

¹⁴⁹ 5 U.S.C. 552a(c), 552a(o)(1)(D), 552a(o)(1)(G), and 552a(o)(1)(K); OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30; OMB Circular A-130, Appendix I, at 4(d).

¹⁵⁰ 5 U.S.C. 552a(m)(1).

¹⁵¹ 5 U.S.C. 552a(m)(1).

¹⁵² 5 U.S.C. 552a(m)(1).

¹⁵³ 5 U.S.C. 552a(b), 552a(j), 552a(k), 552a(m), 552a(o), 552a(p), 552a(q), and 552a(v); OMB Circular A-130, Appendix I, at 3(a); 47 CFR §§ 0.555(b) and 0.561.

¹⁵⁴ 5 U.S.C. 552a(e)(9) – (e)(10), 552a(m), 552a(o)(1)(F) – (o)(1)(I).

- (3) Contractor personnel involved in the matching program shall be made explicitly aware of their obligations under the Privacy Act and of these guidelines, and any special safeguards in relation to each specific match performed;¹⁵⁵
 - (4) Any **disclosures** of records by the FCC to the contractor should be made pursuant to a **routine use provision** of the Privacy Act.¹⁵⁶
- 11-16. OMB Guidance. OMB has published guidelines that are intended to help Federal agencies relate the procedural requirements of the Privacy Act, as amended by Pub. L. 100-503, the *Computer Matching and Privacy Protection Act of 1988*, (“Computer Matching Act”) 54 FR 25818, with the operational requirements of automated matching programs.¹⁵⁷ Complying with OMB’s Guidelines does not relieve a Federal agency of its obligations to comply with the provisions of the Privacy Act, including any provisions not cited in these Guidelines.¹⁵⁸
- 11-17. Miscellaneous Matching Activities. In the Data Integrity Board’s annual report, as required under 5 U.S.C. 552a(u)(3)(D), the Board may report the Commission’s matching activities that are not matching programs on an aggregate basis, if and to the extent necessary, to protect ongoing law enforcement or counterintelligence investigations.¹⁵⁹
- 11-18. Annual Matching Activity Report. The Privacy Act, 5 U.S.C. 552a(u)(3)(D), and OMB regulations require that the DIB of each agency compile a *Annual Matching Activity Report*, which is submitted to OMB at privacy-oira@omb.eop.gov by June 1 and posted on the FCC’s website at <https://www.fcc.gov/general/privacy-act-information>.
- (A) The purpose of this report is to inform the Chairman of the FCC and OMB about the matching programs in which the Commission has participated for the previous calendar year.¹⁶⁰
 - (B) The DIB’s annual matching activity report shall include the following elements:¹⁶¹
 - (1) Current information about the composition of the DIB, including:¹⁶²
 - (a) A list of the names and positions of the DIB members;¹⁶³

¹⁵⁵ 5 U.S.C. 552a(m), 552a(o), and 552a(q).

¹⁵⁶ 5 U.S.C. 552a(b), 552a(j), 552a(k), 552a(m), 552a(o), and 552a(q); 47 CFR §§ 0.555(b) and 0.561.

¹⁵⁷ CITE

¹⁵⁸ CITE

¹⁵⁹ 5 U.S.C. 552a (u)(6).

¹⁶⁰ 5 U.S.C. 552a(u)(3)(D); OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30; (2016), at 29-30; OMB Circular A-130, Appendix I, at 3(a)(5) and 4(b).

¹⁶¹ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶² OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶³ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

- (b) The name and contact information of the DIB secretary;¹⁶⁴ and
 - (c) Any changes in the DIB's membership or structure that occurred during the year.¹⁶⁵
- (2) A list of each matching program in which the agency participated during the year. For each matching program, the report shall include:¹⁶⁶
 - (a) A brief description of the matching program, including the names of all participating Federal and non-Federal agencies;¹⁶⁷
 - (b) Links to the matching notice and matching agreement posted on the agency's website at <https://www.fcc.gov/general/privacy-act-information>;¹⁶⁸
 - (c) An account of whether the agency has fully adhered to the terms of the matching agreement;¹⁶⁹
 - (d) An account of whether all disclosures of agency records for use in the matching program continue to be justified;¹⁷⁰ and
 - (e) An indication of whether a cost-benefit analysis was performed, the results of the cost-benefit analysis, and an explanation of why the agency proceeded with any program for which the results of the cost-benefit analysis were unfavorable.¹⁷¹
- (3) For each matching program for which the DIB waived the cost-benefit analysis requirement, the reasons for the waiver.¹⁷²

¹⁶⁴ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶⁵ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶⁶ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶⁷ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶⁸ OMB Circular A-108 OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁶⁹ OMB Circular A-108 (2016) OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁷⁰ OMB Circular A-108 (2016) OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁷¹ OMB Circular A-108 (2016), OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁷² OMB Circular A-108 (2016) OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

- (4) A description of any matching agreement that the DIB disapproved and the reasons for the disapproval.¹⁷³
- (5) A description of any violations of matching agreements that have been alleged or identified, and a discussion of any action taken in response.¹⁷⁴
- (6) A discussion of any litigation involving the agency's participating in a matching program.¹⁷⁵
- (7) For any litigation based on allegations of inaccurate records, an explanation of the steps that the agency used to ensure that integrity of its records as well as the verification process it used in the matching program.¹⁷⁶
- (8) A review, when appropriate, of any matching agency activities that the DIB approved and/or reviewed, which are not matching programs, *e.g.*, data sharing arrangements.¹⁷⁷

¹⁷³ OMB Circular A-108 (2016) OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁷⁴ OMB Circular A-108 (2016) OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁷⁵ OMB Circular A-108 (2016), at 29.

¹⁷⁶ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

¹⁷⁷ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 29-30.

CHAPTER 12

FEDERAL AGENCY WEBSITES PRIVACY POLICIES

- 12-1 Policy. The webpages of the FCC and other Federal agencies are a speedy and important tool to disseminate information about the FCC's mission, policies, and programs when the public visits these webpages.¹
- (A) The FCC website is provided as a public service to inform to the public in a timely, equitable, efficient, and appropriate manner and to maintain inventories of information about the Commission's regulatory mission, activities, and services.²
 - (B) The FCC's privacy policies and practices governing its webpages comply with OMB privacy policy guidelines and requirements.³
 - (C) Therefore, it is the FCC's policy to protect the privacy of everyone who visits these webpages. Users are not required to provide any personally identifiable information (PII) when entering and browsing.⁴
- 12-2. Definitions.
- (A) **Web measurement and customization technologies** are technologies used to remember a user's online interactions with a website or online applications in order to conduct measurement and analysis of usage or to customize the user's experience.⁵
 - (B) **Single-session technologies** are technologies that remember a user's online interactions within a single session or visit. Any identifier correlated to a particular user is used only within that session, is not later reused, and is deleted immediately after the session ends.⁶
 - (C) **Multi-session technologies** are technologies that remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier for each user, which lasts across multiple sessions or visits.⁷
- 12-3. Federal Website Guidelines. Federal agencies are required to manage their websites in accordance with Federal statutes, requirements, and OMB policies.⁸

¹ OMB Memorandum M-99-18, "Privacy Policies on Federal Web Sites," June 2, 1999, at 1.

² OMB Memorandum M-05-04, Attachment, at 1; OMB Circular A-130; Paperwork Reduction Act.

³ OMB Memorandum M-99-18 Attachment, at 1.

⁴ FCC Privacy Policy website; OMB Memorandum M-03-22, Attachment A, at 7.

⁵ OMB Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies," June 25, 2010, Attachment 1, at 3.

⁶ OMB Memorandum M-10-22, Attachment 1, at 4.

⁷ OMB Memorandum M-10-22, Attachment A, at 4.

⁸ OMB Memorandum M-05-04, Attachment, at 1(A).

- (A) Federal agency public websites are information resources funded in whole or in part by the Federal Government and operated by a Federal agency, contractor, or other organization on behalf of the agency.⁹
- (B) Federal agencies are required to disseminate information to the public in a timely, equitable, efficient and appropriate manner and to maintain inventories of information dissemination products.¹⁰
- (C) Federal agencies are expected to protect the privacy of information about members of the public who visit their website.¹¹
- (D) Federal agency should include a search function at the principal public website and any major entry points.¹²
- (E) Federal agencies must establish and enforce agency-wide linking policies that describe management controls for linking within and beyond the agency to protect the privacy of users.¹³

12-4. Federal Website Information Collection Practices. Federal agencies must alert visitors as to whether and what kinds of information the website collects.

- (A) Federal agencies must inform visitors about any “automatically collected information” that is not subject to the Privacy Act. This information may include:
 - (1) The user’s IP address,
 - (2) The location and time of visit, and
 - (3) The identity of the use(s) for which this information is being collected, *e.g.*, site management or security purposes.¹⁴
- (B) Federal agency websites that collect personally identifiable information (PII) are subject to the requirements of the Privacy Act.
- (C) When collecting PII from their official agency website, the Federal agency must explain what portion of the PII is maintained and retrieved by name or personal identifier (*i.e.*, PII) in a system of records and provide a **Privacy Act Notice** either:¹⁵
 - (1) At the point of collection (*e.g.*, on the website or webpage);¹⁶ or

⁹ OMB Memorandum M-05-04, at 1.

¹⁰ OMB Memorandum M-05-04, Attachment, at 1(B).

¹¹ OMB Memorandum M-05-04, Attachment, at 2; OMB Memorandum M-03-22; OMB Circular A-130, at Appendix I.

¹² OMB Memorandum M-05-04, Attachment, at 5(B).

¹³ OMB Memorandum M-05-04, Attachment, at 5(3).

¹⁴ OMB Memorandum M-03-22, at III.2.a(iii).

¹⁵ OMB Memorandum M-03-22, at III(D)(2)(a)(i).

¹⁶ OMB Memorandum M-03-22, at III(D)(2)(a)(i)(1).

- (2) Via a link to the agency's general privacy policy.¹⁷

12-5. Federal Website Privacy Act Notice. Federal agencies are required to post a **Privacy Act Notice** on their website to inform users to the site when the website collects PII.¹⁸

- (A) The Privacy Act Notice is the single, centrally located statement that provides a clear explanation of the agency's general privacy-related practices that pertain to the official webpages and other on-line activities.¹⁹
- (B) The Privacy Act Notice must notify the visitor to the agency's official website concerning the Privacy Act's requirements that govern the collection of this PII:²⁰
 - (1) The Authority for the collection of the information;²¹
 - (2) What information is being collected;²²
 - (3) The purposes and/or intended use(s) for why the collection of this information;²³
 - (4) With whom the information will be shared;²⁴
 - (5) Whether providing the information is mandatory or voluntary;²⁵
 - (6) The effects of not providing all or any part of the requested information;²⁶
 - (7) What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;²⁷
 - (8) How the agency's privacy policy will secure and protect the information.²⁸
 - (9) The rights of the individual under the Privacy and other laws relevant to the protection of the privacy of the individual;²⁹ and

¹⁷ OMB Memorandum M-03-22, at III(D)(2)(a)(i)(2).

¹⁸ OMB Memorandum M-03-22, at III(E); OMB Memorandum M-05-04, at 3(F).

¹⁹ OMB Memorandum M-99-18, at 1.

²⁰ OMB Memorandum M-03-22, at III(D)(2)(a)(ii); OMB Memorandum M-05-04, Attachment, at 1; OMB Memorandum M-99-18, at 1; OMB Memorandum M-10-22, Attachment A, at 7; OMB

²¹ OMB Memorandum M-03-22, at III(D)(2)(a)(ii); OMB Memorandum M-05-04, Attachment, at 1; OMB Memorandum M-99-18, at 1; OMB Memorandum M-10-22, Attachment A, at 7; OMB.

²² OMB Memorandum M-03-22, Attachment B, at 16-17.

²³ OMB Memorandum M-03-22, at III(D)(2)(a)(ii); OMB Memorandum M-05-04, Attachment, at 1; OMB Memorandum M-99-18, at 1; OMB Memorandum M-10-22, Attachment A, at 7; OMB

²⁴ OMB Memorandum M-03-22, at 16-17.

²⁵ OMB Memorandum M-03-22, at III(D)(2)(a)(ii); OMB Memorandum M-05-04, Attachment, at 1; OMB Memorandum M-99-18, at 1; OMB Memorandum M-10-22, Attachment A, at 7; OMB

²⁶ OMB Memorandum M-03-22, at III(D)(2)(a)(ii); OMB Memorandum M-05-04, Attachment, at 1; OMB Memorandum M-99-18, at 1; OMB Memorandum M-10-22, Attachment A, at 7; OMB.

²⁷ OMB Memorandum M-03-22, at 16-17.

²⁸ OMB Memorandum M-03-22, Attachment A, at 8; OMB Memorandum M-05-04, Attachment, at 1; OMB Memorandum M-99-18, at 1.

²⁹ OMB Memorandum M-03-22, at 16-17.

- (10) The link for public comment, and other, miscellaneous links to assist the public.³⁰
- (C) The Federal agency must also include in its Privacy Act Notice the agency's privacy policy that:
 - (1) Informs visitors whenever providing requested information is voluntary;³¹
 - (2) Informs visitors how to grant consent for use of voluntarily-provided information;³² and
 - (3) Informs visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.³³
- (D) The Privacy Act Notice governs the website's usage, even if a particular webpage on that Federal agency's website does not collect any PII or other similar information, which may result in creating a Privacy Act record or records, *i.e.*, PII under the Privacy Act.³⁴
- (E) The Privacy Notice must be clearly labeled and easily accessible when someone visits the website³⁵ so that visitors to the site know the website's information practices,³⁶ and that the "cookies" on this website do not retain any information about visitors once they have left it.³⁷
- (F) Federal agencies should post their **Privacy Act Notice** explaining their website privacy policies at:³⁸
 - (1) Their principal website;³⁹
 - (2) Any known, major entry points to their sites;⁴⁰
 - (3) Any webpage that collects substantial information in identifiable form, *i.e.*, PII.⁴¹
- (G) The Federal agency's privacy act notice should be:

³⁰ OMB Memorandum M-05-04, Attachment, at 1.

³¹ OMB Memorandum M-10-22, Attachment A, at 7; OMB Memorandum M-03-22, at III.D.1(a)(i).

³² OMB Memorandum M-10-22, Attachment A, at 7; OMB Memorandum M-03-22, at III.D.1(a)(ii).

³³ OMB Memorandum M-10-22, Attachment A, at 7; OMB Memorandum M-03-22, at III.D.1(a)(iii).

³⁴ OMB Memorandum M-99-18, Attachment A, at 1.

³⁵ OMB Memorandum M-99-18, Attachment A, at 1.

³⁶ OMB Memorandum M-99-18, Attachment A, at 1.

³⁷ OMB Memorandum M-99-18, Attachment A, at 2.

³⁸ OMB Memorandum M-03-22, at III(E); OMB Memorandum M-05-04, at 3(F).

³⁹ OMB Memorandum M-03-22, at III(E)(1).

⁴⁰ OMB Memorandum M-03-22, at III(E)(2).

⁴¹ OMB Memorandum M-03-22, at III(E)(3).

- (1) Clearly labeled and easily accessible;⁴²
- (2) Written in plain language;⁴³ and
- (3) Made clear and easy to understand whether by:
 - (a) Integrating all information and statements into a single posting,⁴⁴
 - (b) Layering a short “highlights” notice linked to the full explanation,⁴⁵ or
 - (c) Other means the agency determines is effective.⁴⁶
- (H) Federal agencies must notify website visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies:⁴⁷
 - (1) In the body of their web privacy policy that enumerates that information that may be collected;⁴⁸
 - (2) Via a link to the applicable agency regulations *e.g.*, Privacy Act regulation and pertinent system notice;⁴⁹ or
 - (3) Via a link to other official summary statutory rights, such as the summary of the Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov, or other Federal regulations that would apply specifically to the FCC regulatory responsibilities.⁵⁰

12-6. Information Sharing. Federal agencies may share information from visitors to their websites under certain conditions.

- (A) A Federal agency must insure that they do not engage in “information sharing” with other agencies unless the agency notifies visitors that it engages in such practices and that any data sharing fully protects the privacy of individuals, including compliance with the Privacy Act and all other applicable privacy laws, regulations, and policies.⁵¹

⁴² OMB Memorandum M-03-22, at III(F)(1).

⁴³ OMB Memorandum M-03-22, at III(F)(2).

⁴⁴ OMB Memorandum M-03-22, at III(F)(3).

⁴⁵ OMB Memorandum M-03-22, at III(F)(3).

⁴⁶ OMB Memorandum M-03-22, at III(F)(3).

⁴⁷ OMB Memorandum M-03-22, Attachment A, at 7.

⁴⁸ OMB Memorandum M-03-22, Attachment A, at 7.

⁴⁹ OMB Memorandum M-03-22, Attachment A, at 7-8.

⁵⁰ OMB Memorandum M-03-22, Attachment A, at 8.

⁵¹ OMB Memorandum M-11-02, “Sharing Data While Protecting Privacy,” November 3, 2010, at 1.

- (B) Federal agency's Internet privacy policies may include an advisory notice that collected information from its website may be shared and protected as necessary for authorized law enforcement, homeland security, and national security activities.⁵²
- 12-7. Computer Security. Federal agencies should comply with all requirements for computer security in administering their websites and post the following information in their privacy policy guidelines should include:⁵³
- (A) In clear language, information about management, operational, and technical controls that ensure the security and confidentiality of PII records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.);⁵⁴ and
 - (B) In general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)⁵⁵
- 12-8. Privacy Impact Assessments (PIA) and Systems of Records. The Privacy Act and OMB regulations require that Federal agencies must:
- (A) Conduct a **PIA** or **adapted PIA** for their website and post it on their privacy webpage.⁵⁶ See Chapter 9 and Addendum 2: "PIA" and Addendum 3: "Adapted PIA."
 - (B) Create a new **system of records** or update an existing system of records if the PIA or adapted PIA determines that the website is collecting PII, as required under 5 U.S.C. 552a(e).⁵⁷ See Chapter 6 and Addendum 1: "System of Records Notice."
- 12-9. Machine Readable Technologies. Federal agencies must adopt machine readable technology that alerts website users automatically about whether website privacy practices match their personal privacy preferences.⁵⁸
- (A) Federal agencies must also be cognizant about using web technology to track the activities of users over time and across different web sites.⁵⁹
 - (B) Federal agencies and contractors (when operating web sites on behalf of agencies) may only use web detection devices, technologies, and applications like "cookies," when they provide clear and conspicuous notices on their websites and when the following conditions are met:⁶⁰

⁵² OMB Memorandum M-11-02, "Sharing Data While Protecting Privacy," November 3, 2010, at 1; OMB Memorandum M-03-22, Attachment A, at 9. CHECK sites.

⁵³ OMB Memorandum M-03-22, Attachment A, at 9; OMB Memorandum M-99-18, at 2.

⁵⁴ OMB Memorandum M-03-22, Attachment A, at 9.

⁵⁵ OMB Memorandum M-03-22, Attachment A, at 9.

⁵⁶ OMB Memorandum M-10-23, at 1; OMB Memorandum M-03-22, at Attachments B. and C; OMB Memorandum M-10-22.

⁵⁷ 5 U.S.C. 552a(e);

⁵⁸ OMB Memorandum M-03-22, Attachment A, at 9.

⁵⁹ OMB Memorandum M-05-04, Attachment, at 1.

⁶⁰ OMB Memorandum M-05-04, Attachment, at 2.

- (1) There is a compelling need to gather data on the site;⁶¹
- (2) There are appropriate and publicly disclosed privacy safeguards for handling information derived from “cookies”;⁶² and
- (3) The agency head, i.e., FCC Chairman, has approved this policy.⁶³
- (C) Such technology enables users to make an informed choice about whether to conduct business with that site.⁶⁴
- (D) Agencies may choose to adopt other privacy protective tools that become available as the technology advances.⁶⁵
- (E) Agencies must adopt a timetable for translating their privacy policies into a standardized machine-readable format.⁶⁶

12-10. Federal Website Exclusions. These Federal privacy requirements exclude:

- (A) Information other than “government information” as defined in OMB Circular A-130;⁶⁷
- (B) Federal Intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);⁶⁸ and
- (C) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology under Section 202(i) of the *E-Government Act*.⁶⁹

12-11. Webpage Measurement and Customization. Federal agencies may use web measurement and customization technologies for the purposes of improving their agencies’ services online by conducting measurement and analysis of usage or by customizing the user’s experience.⁷⁰

- (A) There are potential benefits for Federal agencies from various web measurement and customization technologies may allow Federal agencies.
 - (1) To customize their settings, avoid filling out duplicative information, and navigate websites more quickly and in a way that serves their interests and needs.⁷¹

⁶¹ OMB Memorandum M-05-04, Attachment, at 2.

⁶² OMB Memorandum M-05-04, Attachment, at 2.

⁶³ OMB Memorandum M-05-04, Attachment, at 2.

⁶⁴ OMB Memorandum M-03-22, Attachment A, at 9.

⁶⁵ OMB Memorandum M-03-22, Attachment A, at 9.

⁶⁶ OMB Memorandum M-03-22, Attachment A, at 9.

⁶⁷ OMB Memorandum M-03-22, at III(C)(1).

⁶⁸ OMB Memorandum M-03-22, at III(C)(2).

⁶⁹ OMB Memorandum M-03-22, at III(C)(3).

⁷⁰ OMB Memorandum M-10-22, Attachment 1, at 4.

⁷¹ OMB Memorandum M-10-22, at 1.

- (2) To see what is useful to the public and respond accordingly, providing better service to customers and users.⁷²
- (B) Federal agencies must also be cognizant of the potential privacy impacts concerning the use of web technology to track the activities of users over time and across different web sites.⁷³
- (C) Federal agencies and contractors (when operating web sites on behalf of agencies) may only use web detection devices, technologies, and applications like “cookies,” when they provide clear and conspicuous notices on their websites and when the following conditions are met:⁷⁴
 - (1) There is a compelling need to gather data on the site;⁷⁵
 - (2) There are appropriate and publicly disclosed privacy safeguards for handling information derived from “cookies”;⁷⁶ and
 - (3) The agency head, i.e., FCC Chairman, has approved this policy.⁷⁷
- (D) Federal agencies must be aware of and sensitive to the unique privacy questions raised by the government’s use of such technologies.⁷⁸
 - (1) Any such uses must not compromise or invade personal privacy.⁷⁹
 - (2) It is important, therefore, to provide clear, firm, and unambiguous protection against any uses that would compromise or invade personal privacy.⁸⁰
- (E) Federal agencies may not use certain webpage measurement and customization technologies that:⁸¹
 - (1) Track user individual-level activity on the Internet outside of the Commission’s website or applications from which the technology originates;⁸²
 - (2) Share the data obtained through such technologies, without the user’s explicit consent, with other entities, *e.g.*, other Federal agencies;⁸³

⁷² OMB Memorandum M-10-22, at 1.

⁷³ OMB Memorandum M-05-04, Attachment, at 1.

⁷⁴ OMB Memorandum M-05-04, Attachment, at 2.

⁷⁵ OMB Memorandum M-05-04, Attachment, at 2.

⁷⁶ OMB Memorandum M-05-04, Attachment, at 2.

⁷⁷ OMB Memorandum M-05-04, Attachment, at 2.

⁷⁸ OMB Memorandum M-10-22, June 25, 2010, at 2.

⁷⁹ OMB Memorandum M-10-22, June 25, 2010, at 2.

⁸⁰ OMB Memorandum M-10-22, June 25, 2010, at 2.

⁸¹ OMB Memorandum M-10-22, Attachment 1, at 4.

⁸² OMB Memorandum M-10-22, Attachment 1, at 4.

⁸³ OMB Memorandum M-10-22, Attachment 1, at 4.

- (3) Cross-reference, without the user's explicit consent, any data gathered from web measurement and customization technologies against PII to determine individual-level online activity;⁸⁴
 - (4) Collect PII without the user's explicit consent in any fashion;⁸⁵ or
 - (5) Allow any other uses that OMB may designate as prohibited uses.⁸⁶
- (F) The appropriate web measurement and customization technologies are divided into three **Usage Tiers**:
- (1) **Tier 1 – single session** encompasses any use of single session web measurement and customization technologies.⁸⁷
 - (2) **Tier 2 – multi-session without PII** encompasses any use of multi-session web measurement and customization technologies when no PII is collected (including when the Commission is unable to identify an individual as a result of its use of such technologies).⁸⁸
 - (3) **Tier 3 – multi-session with PII** encompasses any use of multi-session web measurement and customization technologies when PII is collected (including when the Commission is able to identify an individual as a result of its use of such technologies).⁸⁹

12-12. Clear Notice and Personal Choice Requirements. Federal agencies may not use web measurement and customization technologies from which it is not easy for the public to opt-out.⁹⁰

- (A) Federal agencies should provide users in its web privacy policies with the Commission's policy to enable web measurement and customization technologies by default or not, which requires users to make an "opt-out" or "opt-in" decision.⁹¹
- (B) Federal agencies should provide information to users who decline to opt-in or decide to opt-out with access to information that is compatible to the information available to users who opt-in or decline to opt-out.⁹²
- (C) OMB regulations provide the FCC with three options:
 - (1) **Agency side opt-out** – An agency is encouraged and authorized, where appropriate, to use web tracking and measurement technologies in order to

⁸⁴ OMB Memorandum M-10-22, Attachment 1, at 4.

⁸⁵ OMB Memorandum M-10-22, Attachment 1, at 4.

⁸⁶ OMB Memorandum M-10-22, Attachment 1, at 4.

⁸⁷ OMB Memorandum M-10-22, Attachment 1, at 5.

⁸⁸ OMB Memorandum M-10-22, Attachment 1, at 5.

⁸⁹ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁰ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹¹ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹² OMB Memorandum M-10-22, Attachment 1, at 5.

remember that a user has opted out of all other uses of such technologies on the relevant domain or applications. Such uses are considered Tier 2.⁹³

- (2) **Client side opt-out** – If an agency side opt-out mechanisms are not appropriate or available, instructions on how to enable client side opt-out mechanisms may be used.⁹⁴
 - (a) Client side opt-out mechanisms allow the user to opt out of web measurement and customization technologies by changing the settings of a specific application or program on the user’s local computer.⁹⁵
 - (b) Users, for example, may be able to disable persistent cookies by changing the settings on commonly used web browsers.
 - (c) Users may access this site: http://www.usa.gov/optout_instructions.shtml to obtain general instructions on how to opt out of some of the most commonly used web measurement and customization technologies.⁹⁶
- (3) **Tier 3 restrictions** – An agency employing Tier 3 uses must use opt-in functionality.⁹⁷

Note: The requirement is stated plainly in the FCC’s web privacy policy at:⁹⁸ <http://www.fcc.gov/fccprivacypolicy.html>.

12-13. Web Measurement and Customization Technologies. Federal agencies may use web measurement and customization technologies subject to certain privacy requirements:⁹⁹

- (A) Tier 1 and Tier 2 uses are allowed so long as the agency is in compliance with OMB policies and guidelines.¹⁰⁰
- (B) The agency must provide clear and conspicuous notice in the agency’s on-line Privacy Act Notice’s privacy policy and cite the use of such technologies.¹⁰¹
- (C) Each Federal agency must comply with its own internal policies governing the use of such technologies.¹⁰²

⁹³ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁴ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁵ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁶ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁷ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁸ OMB Memorandum M-10-22, Attachment 1, at 5.

⁹⁹ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁰ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰¹ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰² OMB Memorandum M-10-22, Attachment 2, at 7.

12-14. Tier 3 Technologies. Federal agencies must add additional privacy protections when using Tier 3 web measurement and customization technologies.¹⁰³

(A) Any proposals to engage in Tier 3 technologies uses must be reviewed by the agency's SAOP.¹⁰⁴

(B) For new proposals of Tier 3 uses or substantive changes to existing uses of such technologies, the Federal agency must:

(1) Solicit comment through the agency's Open Government webpage at for a minimum of 30 days.¹⁰⁵

Note: The FCC's policy are found at: www.fcc.gov/open

(2) The notice in the *Federal Register* must also:

(a) Include the agency's proposal to use such technologies;¹⁰⁶ and

(b) Provide a description for how the agency will use the technologies.¹⁰⁷

(3) Each agency must review and consider substantive comments and make changes to the proposed uses of the technologies as appropriate.¹⁰⁸

(C) The CIO may provide a written exemption from the "notice and comment" requirement, if it is reasonably determined likely to result in serious public harm.¹⁰⁹

(D) Any proposals to use Tier 3 technologies must also have the explicit written approval of the CIO. This approval must be cited in the agency's on-line privacy policy.¹¹⁰

(E) The agency may only be authorized to use Tier 3 web measurement and customization technologies after its CIO has given approval and after the notice and comment period ends.¹¹¹

(F) OMB will only grant permission to use web measurement and customization technologies if they conform to the process and/or parameters in these guidelines.¹¹²

(G) Federal agencies that are not in compliance with OMB guidelines on web measurement and customization technologies must cease use of such technologies and inform OMB of

¹⁰³ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁴ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁵ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁶ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁷ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁸ OMB Memorandum M-10-22, Attachment 2, at 7.

¹⁰⁹ OMB Memorandum M-10-22, Attachment 2, at 7.

¹¹⁰ OMB Memorandum M-10-22, Attachment 2, at 7.

¹¹¹ OMB Memorandum M-10-22, Attachment 2, at 7.

¹¹² OMB Memorandum M-10-22, Attachment 2, at 8.

the extent of such unauthorized use. OMB will provide the necessary and appropriate guidance.¹¹³

12-15. Privacy Requirements for Tier 3 Technologies. Federal agencies must add these online privacy policy requirements for Tier 3 web measurement and customization technologies:¹¹⁴

- (A) The purpose of the web measurement and/or customization technology;¹¹⁵
- (B) The usage Tier, session type, and technology used;¹¹⁶
- (C) The nature of the information collected;¹¹⁷
- (D) The purpose and use of the information;¹¹⁸
- (E) Whether and to whom the information will be disclosed;¹¹⁹
- (F) The privacy safeguards applied to the information;¹²⁰
- (G) The data retention policy for the information;¹²¹
- (H) Whether the technology is enabled by default or not and why;¹²²
- (I) How to opt-out of the web measurement and/or customization technology;¹²³
- (J) A statement that opting-out still permits users to access comparable information or services;¹²⁴ and
- (K) The identities of all third-party vendors involved in the measurement and customization process.¹²⁵

12-16. Data Safeguarding and Privacy. Federal agencies' uses of web measurement and customization technologies must:

- (A) Comply with existing privacy policies and data safeguard standards.¹²⁶

¹¹³ OMB Memorandum M-10-22, Attachment 2, at 8.

¹¹⁴ OMB Memorandum M-10-22, Attachment 2, at 7 and Attachment 3, at 9.

¹¹⁵ OMB Memorandum M-10-22, Attachment 3, at 9.

¹¹⁶ OMB Memorandum M-10-22, Attachment 3, at 9.

¹¹⁷ OMB Memorandum M-10-22, Attachment 3, at 9.

¹¹⁸ OMB Memorandum M-10-22, Attachment 3, at 9.

¹¹⁹ OMB Memorandum M-10-22, Attachment 3, at 9.

¹²⁰ OMB Memorandum M-10-22, Attachment 3, at 9.

¹²¹ OMB Memorandum M-10-22, Attachment 3, at 9.

¹²² OMB Memorandum M-10-22, Attachment 3, at 9.

¹²³ OMB Memorandum M-10-22, Attachment 3, at 9.

¹²⁴ OMB Memorandum M-10-22, Attachment 3, at 9.

¹²⁵ OMB Memorandum M-10-22, Attachment 3, at 9.

¹²⁶ OMB Memorandum M-10-22, Attachment 1, at 5.

- (B) A PIA and/or SORN may be required for the webpage and/or website to insure that these comply with the agency's privacy requirements, and these should cite the applicable policies.¹²⁷

12-17. Third Party Websites. If Federal agencies use a website or application hosted on a third-party site using web measurement and customization technologies to which Federal privacy and data safeguarding standards do not apply, the agency provide the public with alternatives for acquiring comparable information and services.¹²⁸

- (A) Provide an official Federal agency website to learn about the agency's activities and/or to communicate with the agency without having to join a third party social media website;¹²⁹ and
- (B) Provide also an alternative, official government e-mail address where users can communicate with the agency, send feedback, and/or solicit comments about its programs and activities in addition to using the third party website to solicit feedback.¹³⁰

Note: The regulations governing privacy policies for using third party webpages are explained in Chapter 13.

12-18. Data Retention and Access Limits. Federal agencies may retain data collected from web measurement and customization technologies for only as long as necessary to achieve the specific objective for which it was collected.¹³¹

- (A) The time frame for retention of data must be both limited and correlated to a specific objective. If not required by law, policy, or a specific need for web measurement or customization objective, the FCC should limit the retention of such data to one year or less.¹³²
- (B) Information collected from web measurement and customization technologies, which is determined to be a "Federal Record," must comply with the appropriate Federal Records Act regulations for records retention and disposal.¹³³
 - (1) General Records Schedule 20 (GRS 20) pertains to Electronic Records; specifically, the disposition authority cited in General Records Schedule 20 Item 1C "Electronic Records" ("Files /Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records – Electronic files ... created to monitor system usage...") is applicable to information collected from web measurement and customization technologies.¹³⁴

¹²⁷ OMB Memorandum M-10-22, Attachment 1, at 5.

¹²⁸ OMB Memorandum M-10-22, Attachment 1, at 6.

¹²⁹ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³⁰ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³¹ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³² OMB Memorandum M-10-22, Attachment 1, at 6.

¹³³ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³⁴ National Archives and Records Administration (NARA), *Electronic Records, General Records Schedule 20* (2010), available at <http://www.archives.gov/records-mgmt/grs/grs20.html>.

- (2) Use of GRS 20 is mandatory for those categories of electronic records described in the schedule unless the agencies have requested an alternative disposition authority from NARA.¹³⁵

12-19. Safety and Security of PII. Federal agencies should enforce safety and security protocols to protect the PII that the agency's website or application collects to guard against data breaches.

- (A) Access to the PII data should be limited to employees and contractors who require access as part of their job duties and responsibilities;¹³⁶
- (B) To the extent feasible, technical enforcement mechanisms should be put in place to implement stated retention times and to limit access to authorized personnel;¹³⁷ and
- (C) Where technical enforcement mechanisms are not feasible, policy or contractual enforcement mechanisms must be present.¹³⁸

12-20. Verification. Federal agencies using web measurement and customization technology must:¹³⁹

- (A) Conduct an annual review of the Commission's systems and procedures to demonstrate this compliance;¹⁴⁰ and
- (B) Post the results of this review on the agency's "/open" page with a mechanism for the public to provide feedback on the results of this review.¹⁴¹

Note: FCC's webpage link: <https://www.fcc.gov/general/consumer-information-registry-fcc>

12-21. Children's On-line Privacy Protection Act (COPPA). All Federal websites and contractors operating on behalf of Federal agencies must comply with the standards set forth in the *Children's On-line Privacy Protection Act of 1998* (COPPA) with respect to the collection of PII online at websites directed to children.¹⁴²

- (A) The FCC adheres to COPPA in regards to access by children younger than 13 years of age to the Commission's websites as explained on the FCC's website at: <http://www.fcc.gov/fccprivacypolicy.html>.¹⁴³
- (B) The three hallmarks of COPPA for purposes of Federal on-line activity are:¹⁴⁴

¹³⁵ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³⁶ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³⁷ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³⁸ OMB Memorandum M-10-22, Attachment 1, at 6.

¹³⁹ OMB Memorandum M-10-22, Attachment 1, at 6; OMB Memorandum M-10-06, Dec. 8, 2009.

¹⁴⁰ OMB Memorandum M-10-22, Attachment 1, at 6; OMB Memorandum M-10-06, Dec. 8, 2009.

¹⁴¹ OMB Memorandum M-10-22, Attachment 1, at 6; OMB Memorandum M-10-06, Dec. 8, 2009.

¹⁴² OMB Memorandum M-05-04, Attachment, at 2.

¹⁴³ OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003, at 11.

- (1) Notice of information collection practices;¹⁴⁵
- (2) Agencies whose Internet sites offer a Verifiable parental consent;¹⁴⁶ and
- (3) Access as governed by the Federal Trade Commission's guidelines.¹⁴⁷

12-22. OMB Guidance. OMB recommends that Federal agencies consult OMB for guidance on appropriate design and content for websites.

- (A) OMB guidelines are based on the recommendations and best practices published by the Interagency Committee on Government Information at: <http://www.webcontent.gov>.¹⁴⁸
- (B) OMB monitors Federal websites to insure that agencies comply with these website policies as part of OMB's oversight of agencies' information resource management programs and privacy requirements.¹⁴⁹

12-23. FCC Website Policies. FCC website is part of the Commission's information resources.

- (A) The FCC website presents the information about the Commission's duties, and responsibilities to manage the nation's telecommunications.¹⁵⁰
- (B) The FCC website provides information about the services that the Commission provides to the public which includes:¹⁵¹
 - (1) Links to FCC forms and licensing information, policies, and procedures;¹⁵²
 - (2) Rosters of Commission rules and regulations;¹⁵³
 - (3) Public format to read about the Commission and the activities of the B/Os;¹⁵⁴
 - (4) A link to the Freedom of Information and Privacy (FOIA) request forms;¹⁵⁵
 - (5) A posting or link to the FCC's specific website privacy policies;¹⁵⁶

¹⁴⁸ OMB Memorandum M-05-04, Attachment, at 1.

¹⁴⁹ OMB Memorandum M-05-04, at 1.

¹⁵⁰ OMB Memorandum M-05-04, at 1.

¹⁵¹ OMB Memorandum M-05-04, at 1.

¹⁵² FCC website.

¹⁵³ FCC website.

¹⁵⁴ FCC website.

¹⁵⁵ FCC website; OMB Memorandum M-05-04, Attachment, at 2(F)(3).

¹⁵⁶ FCC website; OMB Memorandum M-05-04, Attachment, at 2(F)(4).

- (6) A link to the Privacy Act documents, *i.e.*, Major Information Systems, Systems of Records Notices (SORNs), Privacy Threshold Analyses, and Privacy Impact Assessments, *etc.*;¹⁵⁷ and
- (7) A link for public comment, and other, miscellaneous links to assist the public.¹⁵⁸

Note: *Appendix 5, FCC Website Privacy Posting Requirements.*

- (C) The FCC does not monitor the use of its website(s)—there are no “cookies” or other electronic detection devices or markers to collect PII about users when they visit the website unless users specifically and knowingly choose to provide such information to the Commission.¹⁵⁹
- (D) The FCC’s information dissemination practices on its websites are there to protect the privacy of members of the public when they visit the FCC websites.¹⁶⁰
- (E) The FCC website does record website usage information automatically.¹⁶¹
- (F) The information the FCC gathers from website users and their website viewing practices does not identify users personally, nor is the information used to track or to record the characteristics of the user.
- (G) The FCC’s webpage privacy policy include the provision of a **Privacy Notice** (or **Privacy Statement**) that informs visitors about the FCC’s information and privacy practices.¹⁶²
- (H) The FCC’s Privacy ACT Notice must be posted (or a link provided to) the FCC privacy policies at:
 - (1) The principal FCC websites: www.fcc.gov;¹⁶³
 - (2) Any known, major entry points to the FCC websites;¹⁶⁴
 - (3) Any webpage(s) that collection substantial PII data;¹⁶⁵ and
 - (4) Provides a “hotlink,” if technical requirements do not allow the policy to be posted on the webpage.¹⁶⁶

¹⁵⁷ FCC Privacy Policy website; OMB Memorandum M-05-04, Attachment, at 3(F).

¹⁵⁸ FCC website; OMB Memorandum M-05-04, Attachment, at 3(F).

¹⁵⁹ FCC Privacy Policy website; OMB Memorandum M-99-18, at 4.

¹⁶⁰ OMB Memorandum M-05-04, Attachment, at 2; OMB Memorandum M-03-22, Sept. 26, 2003.

¹⁶¹ FCC Privacy Policy website; OMB Memorandum M-99-18, at 2.

¹⁶² OMB Memorandum M-99-18, at 1; OMB Memorandum M-05-04, “Policies for Federal Agency Public Websites,” Dec. 17, 2004, at 1 and Attachment, at 1; OMB Memorandum M-03-22, Attachment A, at 10.

¹⁶³ OMB Memorandum M-03-22, Attachment A, at 9.

¹⁶⁴ OMB Memorandum M-03-22, Attachment A, at 9.

¹⁶⁵ OMB Memorandum M-03-22, Attachment A, at 9.

¹⁶⁶ OMB Memorandum M-99-18, Attachment at 1.

- (I) If users provide information to the FCC, the FCC will use the information only to fulfill their requests for information or services.¹⁶⁷
- (J) This website viewing data only are used:
 - (1) To do statistical analyzes;
 - (2) To track website operational problems;
 - (3) To prevent fraud; and
 - (4) To improve the effectiveness, security, and integrity of the website.
- (K) The FCC will disclose the website data it collections only in aggregate form to third parties or as may be required by law.¹⁶⁸
- (L) For each webpage that a user visits, the FCC's privacy policy will notify visitors to the webpage that the FCC collects and stores the following technical information:¹⁶⁹
 - (1) Date and time of access;¹⁷⁰
 - (2) URL address of the FCC webpage visited;¹⁷¹
 - (3) Internet domain and IP address from which the webpage was accessed;¹⁷²
 - (4) Type of browser and operating system used to access this site (if provided by the browser);¹⁷³
 - (5) URL address of the referring page (if provided by the browser);¹⁷⁴
 - (6) Completion or success status of the request for a web page or other on-line item;¹⁷⁵
 - (7) File size of the webpage visited;¹⁷⁶ and
 - (8) Identify the use for which this information is collected, *i.e.*, site management or security purposes.¹⁷⁷

¹⁶⁷ FCC Privacy Policy website; OMB Memorandum M-99-18, at 2; OMB Memorandum M-05-04, at 1.

¹⁶⁸ FCC Privacy Policy website.

¹⁶⁹ FCC Privacy Policy website; OMB Memorandum M-03-22, Attachment A, at 8.

¹⁷⁰ FCC Privacy Policy website.

¹⁷¹ FCC Privacy Policy website.

¹⁷² FCC Privacy Policy website.

¹⁷³ FCC Privacy Policy website.

¹⁷⁴ FCC Privacy Policy website.

¹⁷⁵ FCC Privacy Policy website.

¹⁷⁶ FCC Privacy Policy website.

¹⁷⁷ FCC Privacy Policy website; OMB Memorandum M-03-22, Attachment A, at 8.

- (M) The FCC provides a telephone number and e-mail address for users should they have questions about the FCC's webpage's privacy policies and the FCC's privacy policies in general.¹⁷⁸

¹⁷⁸ OMB Memorandum M-03-22, Attachment C, at 14(A)(2).

CHAPTER 13

THIRD-PARTY WEBSITES AND APPLICATIONS

- 13-1. Policy. Third-party websites and technologies like “social media,” *e.g.*, Twitter, Facebook, YouTube, Flickr, and Web 2.0 or Gov 2.0 applications can provide opportunities for Federal agencies or contactors (on behalf of Federal agencies) to engage the public for the purposes of implementing the *Open Government Initiative*’s principles of openness, transparency, public participation, and collaboration.¹
- (A) Federal agencies must exercise greater vigilance to protect individual privacy when using these websites and applications due to the nature of these technologies;²
 - (B) The Privacy Act, OMB guidance, and other established privacy principles require Federal agencies to exercise vigilance about privacy and PII and to coordinate this supervision through the agency’s SAOP;³
 - (C) Federal agencies should provide individuals with the opportunity to communicate with and/or to receive information about the agency’s services and activities through the agency’s official website or other official means rather than individuals having to join a third-party social media website or application;⁴
 - (D) Federal agencies should use third-party websites and applications as auxiliary or ancillary information sources to supplement each agency’s official website and information sources;⁵ and
 - (E) The FCC, like other Federal agencies, should provide its official website at: www.fcc.gov, and/or an FCC e-mail address (as an official alternative to the third party social media website) where users can also send feedback, in addition to the agency’s use of third-party services to solicit feedback for the agency.⁶
 - (1) The official Federal agency website provides the user with the option to access information without being tracked by the third party that is hosting the agency’s social media website;⁷ and

¹ OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010, at 2; CIO Council, “Privacy Best Practices for Social Media,” July 2013, at 2-3.

² OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010, at 2.

³ OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010, at 2.

⁴ OMB Memorandum M-10-23, at 3.

⁵ OMB Memorandum M-10-23, at 3.

⁶ OMB Memorandum M-10-23, at 3; CIO Council, “Privacy Best Practices for Social Media,” July 2013, at 11.

⁷ CIO Council, “Privacy Best Practices for Social Media,” July 2013, at 11.

- (2) The Federal agency website should include information regarding its web measurement and customization technology policy as part of its website's Privacy Policy.⁸

Note: Social media technologies such as wikis, blogs, and social media networks are especially vulnerable to a wide range of cybersecurity risks and vulnerabilities.⁹

The FCC's policies and best practices concerning cyber security are addressed in the *Cyber Security Policy Directive* FCCINST 1479.

- (F) Federal agencies should consult the OMB privacy officer at: privacy-oira@omb.eop.gov for clarification and guidance if additional assistance is needed to determine the appropriateness and suitability for using these third-party websites and applications.¹⁰

13-2. Definitions.

- (A) **Social Media** are web-based tools, websites, applications and media that connect users and allow them to engage in dialogue, share information, collaborate, and interact.¹¹
 - (1) These sites are also known as **Web 2.0** or **Gov 2.0**.¹²
 - (2) Social media websites are oriented primarily to create a rich and engaging user experience by allowing anyone who uses information also to create it;¹³
 - (3) Users of social media add value to the content and data online, and their interactions with the information, including both collectively and individually, can significantly alter the experiences of subsequent users;¹⁴ and
 - (4) Websites like Twitter, Facebook, YouTube, Flickr, and others make it easy to reach large numbers of people, which makes them an ideal platform for sharing information, starting conversations, and exchanging knowledge within and outside government.¹⁵
- (B) **Third-party websites or applications** are web-based technologies, including "social media" websites, that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernmental entity.¹⁶

⁸ CIO Council, "Privacy Best Practices for Social Media," July 2013, at 11.

⁹ CIO Council, "Privacy Best Practices for Social Media," July 2013, at 11.

¹⁰ OMB Memorandum M-10-23, at 7.

¹¹ CIO Council, "Privacy Best Practices for Social Media," July 2013, at 2.

¹² CIO Council, "Privacy Best Practices for Social Media," July 2013, at 2.

¹³ CIO Council, "Privacy Best Practices for Social Media," July 2013, at 2.

¹⁴ CIO Council, "Privacy Best Practices for Social Media," July 2013, at 2.

¹⁵ CIO Council, "Privacy Best Practices for Social Media," July 2013, at 2.

¹⁶ OMB Memorandum M-10-23, Appendix at 8.

- (1) These technologies are often located on a “.com” website or other location that is not part of an official government domain.¹⁷
 - (2) Third-party applications can also be embedded or incorporated on a Federal agency’s official website.¹⁸
- (C) **Make PII Available** means “to make PII available” means any FCC action that causes PII to become available or accessible to the Commission, whether or not the Commission solicits or collects it.¹⁹
- (1) In general, an individual can make PII available to the Commission (or other Federal agency) when he or she provides, submits, communicates, links, posts, or associates PII while using the website or application.²⁰
 - (2) “Associate” can include activities commonly referred to as “friend-ing,” “following,” “liking,” joining a “group,” becoming a “fan,” and comparable functions.²¹
- (D) **Privacy Policy** refers to a single, centrally located statement that is accessible from the FCC’s official homepage. The Privacy Policy is a consolidated explanation of the FCC’s general privacy-related practices that pertain to its official website and the Commission’s other online activities.²²
- (E) **Privacy Act Notice** refers to a brief description of how the FCC’s Privacy Policies apply in a specific situation. The Privacy Notice should be provided at the FCC’s website on the specific webpage or application where individuals are notified of these privacy policies before they engage the FCC and are given an opportunity to make their PII available to the Commission.²³
- (F) **Situational Awareness** refers to viewing social content on third party websites that is made available to the public, and is not intended to include obtaining access to private networks or interacting on social media sites.²⁴
- (G) **Crowdsourcing** is soliciting data related to a specific topic, idea, or issue from a large population of public users, traditionally online community, who have knowledge of that topic, idea, or issue.²⁵

¹⁷ OMB Memorandum M-10-23, Appendix at 8.

¹⁸ OMB Memorandum M-10-23, Appendix at 8.

¹⁹ OMB Memorandum M-10-23, Appendix at 8.

²⁰ OMB Memorandum M-10-23, Appendix at 8.

²¹ OMB Memorandum M-10-23, Appendix at 8.

²² OMB Memorandum M-10-23, Appendix at 9.

²³ OMB Memorandum M-10-23, Appendix at 9.

²⁴ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 14.

²⁵ CIO Council, “Privacy Best Practices for Social Media, July, 2013, Appendix A, at 14.

- (H) **Malware** are software programs that are designed by hackers to damage or do other unwanted actions to a computer system to gather sensitive information or to gain access to privacy computer systems.²⁶
- (H) **Cookies** are used to identify and customize web pages for a user. There are two kinds of cookies:²⁷
 - (1) A **session cookie** is a line of text that are stored temporarily in a computer's random access memory (RAM), which are never written to a drive and are destroyed as soon as the user closes his/her browser.²⁸
 - (2) A **persistent cookie** is saved to a file on the hard drive and is called up the next time a user visits that website, which lets the website remember what the user was interested in the last time he/she visited the website.²⁹

13-3. Types of Use of Social Media. The main uses of social media to date include:

- (A) Social media websites that allow Federal agencies to communicate and share information with the public about their policies, programs, and activities.³⁰
 - (1) Interactive applications allow Federal agencies to engage in dialogue and collaborate with members of the public. These applications can be broken down into categories based on the mode or method used to disseminate information:³¹
 - (a) Applications used to disseminate video and image content, such as third party media providers like YouTube, Flickr, and Picasa.³²
 - (b) Blogs, microblogs, or other applications that permit entries of commentary, such as Twitter, Goggle Blogger, and Wordpress.³³
 - (c) Social networking applications that facilitate two-way (bi-directional) interaction and networking with the public, such as third party social providers like FaceBook, MySpace, LinkedIn, and GovLoop.³⁴
 - (2) Unidirectional or "push" applications that are used for the purposes of one-way (non-interactive) dissemination of information to the public. These applications include widgets/RSS Feeds and audio/video files.³⁵

²⁶ CIO Council, "Privacy Best Practices for Social Media, July, 2013, Appendix A, at 14.

²⁷ CIO Council, "Privacy Best Practices for Social Media, July, 2013, Appendix A, at 4.

²⁸ CIO Council, "Privacy Best Practices for Social Media, July, 2013, Appendix A, at 4.

²⁹ CIO Council, "Privacy Best Practices for Social Media, July, 2013, Appendix A, at 4.

³⁰ CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 3.

³¹ CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 3.

³² CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 3.

³³ CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 4.

³⁴ CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 4.

³⁵ CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 4.

- (B) Social media websites that allow Federal agencies to enhance “situational awareness.” This allows Federal agencies to monitor social media sites to enhance gather mission-related information from a variety of sources, including “crowdsourcing,” and then communicating that information to the agency’s leadership to inform decision making and responsiveness.³⁶
- (1) Federal agencies with national security, emergency response/management, and disaster recovery responsibilities may benefit most from this use of social media.³⁷
 - (2) Monitoring social media to enhance situational awareness can be done by monitoring publicly available online forums, blogs, public websites, and message boards to gather information related to specific search terms (excluding individual members of the public unless there is an operational need and proper authority), events, or issues, as needed to fulfill the business or mission need.³⁸
- (C) Social media websites that function as an operational tool that Federal agencies may use to collect publicly available information, when permitted by the agency’s legal authorities and mission, for such purposes as:³⁹
- (1) Investigating an individual or company in a criminal, civil, or administrative context to prevent fraud or other illegal activities (including undercover investigations when the agency has legal authority to engage in such investigations).⁴⁰
 - (2) Doing an evaluation to determine whether to grant a benefit or to make an eligibility determination about an individuals.⁴¹
 - (3) Making a personnel determination about an (existing) employee.⁴²
 - (4) Conducting a background investigation on, or adjudicating the security clearance of, a prospective employee. (To the extent possible, an agency must ensure that notice is provided prior to accessing or collecting PII, that consent is obtained, and that the individual is involved in the process. Individuals should not require an applicant to provide access to his/her social media accounts.)⁴³
 - (5) Conducting authorized intelligence activities in accordance with the provisions of Executive Order 12333, as amended.⁴⁴

³⁶ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 4.

³⁷ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 4.

³⁸ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 4.

³⁹ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 5.

⁴⁰ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 5.

⁴¹ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 6.

⁴² CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 6.

⁴³ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 6.

⁴⁴ CIO Council, “Privacy Best Practices for Social Media, July, 2013, at 6.

13-4. **Requirements.** The FCC should adhere to these general requirements for Federal agencies when using third-party websites and/or applications:

- (A) **Third-Party Privacy Policies:** before the Commission uses any third-party website or application to engage with the public, the Commission is required to:⁴⁵
 - (1) Evaluate the third-party's privacy policy and terms of service to determine the risks for using the website or application and whether it is appropriate for the Commission's uses;⁴⁶ and
 - (2) Monitor the website for any changes to the third-party's privacy policy and periodically to reassess the risks for using it.⁴⁷
- (B) **External Links:** if there is a link on the FCC's webpage that leads to a third-party website or any other location that is not part of an official government domain, the Commission must provide an "alert" to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being directed to a non-government website that may have different privacy policies from those of the FCC's official website.⁴⁸
- (C) **Embedded Applications:** if the FCC's webpage incorporates a third-party application or embeds a third-party application on the website or other official government domain, the Commission must:⁴⁹
 - (1) Determine what information, including PII, the embedded application may be collecting from individuals who have posted or accessed this social media website or application;⁵⁰
 - (2) Determine whether this website or application may potentially contain malicious coding;⁵¹
 - (3) Disclose the third-party's involvement;⁵²
 - (4) Disclose that the third-party or application may collect information, including PII, from those using it;⁵³
 - (5) Describe the Commission's activities associated with this third-party or application in the FCC's Privacy Policy;⁵⁴ and

⁴⁵ OMB Memorandum M-10-23, at 3.

⁴⁶ OMB Memorandum M-10-23, at 3; CIO Council, "Privacy Best Practices for Social Media, July, 2013, at 4.

⁴⁷ OMB Memorandum M-10-23, at 3.

⁴⁸ OMB Memorandum M-10-23, at 3; CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 9.

⁴⁹ OMB Memorandum M-10-23, at 3.

⁵⁰ CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 8.

⁵¹ CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 8.

⁵² OMB Memorandum M-10-23, at 3.

⁵³ OMB Memorandum M-10-23, at 3.

⁵⁴ OMB Memorandum M-10-23, at 3.

- (6) The FCC should disclose that it is using this website or application, which may contain embedded applications and that this website or application may contain **malicious coding**. The FCC must disclose this information and describe its use in the Commission's main Privacy Policy, along with the social media website Privacy Policy or Notice.⁵⁵
- (D) **Agency Branding:** in general, the FCC's use of a third-party website or application that is not part of an official government domain, requires that there be the appropriate "branding" to distinguish the Commission's activities from those of the nongovernment actors.⁵⁶
- Note:** OMB recommends that the FCC identify its website by displaying the FCC seal on the profile page of a social media website to indicate that this is an official FCC presence.⁵⁷
- (E) **Information Collection:** if the FCC collects information using a third-party website or application, the information collection activity should be limited to what is "necessary for the proper performance of the Commission's functions and that has practical utility."⁵⁸
- (F) **Senior Agency Approval:** as in each Federal agency, the FCC's senior leadership, including but not limited to the SAOP, CIO, and legal counsel, should have responsibility for determining the Commission's uses of social media to enhance situational awareness and in particular, the collection of PII.⁵⁹

Note: The specific FCC policies and procedures concerning social media are addressed in the *Official Use of Social Media by FCC Bureaus, Offices, and Staff Directive* FCCINST 1440.

- (1) These Commission officials should evaluate the various ways that the FCC would like to use social media and ensure a policy of transparency in the agency's uses of social media, especially those that involve viewing publicly available information to alleviate the public's privacy concerns.⁶⁰
- (2) The Commission should develop and implement **Rules of Behavior** that provide guidance on the appropriate policies and procedures that govern how FCC

⁵⁵ OMB Memorandum M-10-23, at 3.

⁵⁶ OMB Memorandum M-10-22, at 4.

⁵⁷ OMB Memorandum M-10-23, at 4; CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 8.

⁵⁸ OMB Memorandum M-10-23, at 4; OMB Circular A-130, at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/; CIO Council, "Privacy Best Practices for Social Media, July 2013, at 4.

⁵⁹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 5-6.

⁶⁰ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

employees and contractors use social media sites, applications, and technologies.⁶¹

- (a) At a minimum these rules of behavior should govern how and when information can be collected about or from members of the public, including the Commission's policy on allowing comments, viewpoints, and opinions on its social media websites or applications.⁶²
 - (b) **Privacy and security training** for employees and contractors should include instruction on these rules of behavior and related privacy issues concerning the Commission's uses of social media and third party applications.⁶³
 - (c) Training may also include guidance on the **personal use of social media** to help employees and contractors to avoid inadvertently appearing to speak on behalf of the agency, or violating privacy, confidentiality, ethical, criminal, or other restrictions on disclosure of PII or other sensitive information.⁶⁴
- (3) The Commission should include these guidelines and requirements for using social media in its privacy and security awareness training program for employees and contractors to ensure accountability and to mitigate the risks of inappropriate collection or misuse of PII.⁶⁵
 - (4) These Commission officials approve and document all policies, programs, and procedures to cover operational uses due to their sensitivity and to require regular, routine reviews to ensure privacy, policy, and program compliance.⁶⁶
- (G) **PIA or Adapted PIA:** a publicly available PIA or adapted PIA must be done to inform the public to ensure transparency and provide notice on the potential PII collection.⁶⁷
- (H) **Social Media Prohibitions:** when using social media, Federal agencies should not:
- (1) Post information collected about specific individuals;⁶⁸
 - (2) Actively seek to connect with other internal or external personal users;⁶⁹
 - (3) Accept other internal or external personal users' invitations to connect;⁷⁰ or

⁶¹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

⁶² CIO Council, Privacy Best Practices for Social Media, July 2013, at 6 and 9.

⁶³ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

⁶⁴ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

⁶⁵ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

⁶⁶ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

⁶⁷ CIO Council, Privacy Best Practices for Social Media, July 2013, at 5.

⁶⁸ CIO Council, Privacy Best Practices for Social Media, July 2013, at 5.

⁶⁹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 5.

⁷⁰ CIO Council, Privacy Best Practices for Social Media, July 2013, at 5.

- (4) Interact on social media websites.⁷¹
 - (I) Develop operational use policies and procedures that are approved and documented by senior agency leadership (*e.g.*, Commissioners, SAOP, CIO, CSIO, and OGC) to cover operational uses due to their sensitivity and that include regular, routine reviews to ensure privacy and program compliance.⁷²
- 13-4. Social Media Best Practices. The CIO Council privacy guidelines for third party social media websites recommend that Federal agencies should:⁷³
- (5) Limit information collecting to the facts surrounding an event and what is happening, rather than who is either involved or reporting the information, unless the agency has specific legal authority to collect PII when monitoring publicly available sites for “situational awareness” activities;⁷⁴
 - (6) Develop policies outlining specific guidelines on when collecting PII may be legal and appropriate based on an agency’s authorities, and who will be allowed access to the PII.⁷⁵
 - (7) Collect PII only in very limited situations, and only when specifically authorized. Collecting PII may also require creating or updating a SORN to cover this activity.⁷⁶
 - (8) Conduct no searches in social media websites or applications for or by PII unless authorized to do so, and in compliance with the appropriate legal requirements and representations in PIAs and SORNs.⁷⁷
 - (9) Avoid proactively “friending,” “following,” or “liking” or similar activities with public users. However:
 - (1) An agency may accept “friend” requests from public users (exceptions can be made for “friending” other U.S. Federal, state, local, or tribal government agencies, professional associations, or other organizations as appropriate based on each agency’s policies;⁷⁸
 - (2) A statement should be included in the PIA or adapted PIA and on the social media account page to inform users that the acceptance of friend requests does not indicate the agency’s endorsement;⁷⁹

⁷¹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 5.

⁷² CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

⁷³ CIO Council, Privacy Best Practices for Social Media, July 2013, at 4 and 9.

⁷⁴ CIO Council, Privacy Best Practices for Social Media, July 2013, at 4 and 9.

⁷⁵ CIO Council, Privacy Best Practices for Social Media, July 2013, at 4-5.

⁷⁶ CIO Council, Privacy Best Practices for Social Media, July 2013, at 4 and 9.

⁷⁷ CIO Council, Privacy Best Practices for Social Media, July 2013, at 9.

⁷⁸ CIO Council, Privacy Best Practices for Social Media, July 2013, at 9.

⁷⁹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 9.

- (3) Each agency should have policies that address “friending,” “following,” and “liking” users;⁸⁰ and
 - (4) Each agency should adopt names and profiles that are easily identifiable as agency accounts, as well as establish secure passwords so that accounts can only be accessed by administrators.⁸¹
- 13-4. Information Sharing and Retention. Federal agencies using social media to interact with the public or to collect information (*i.e.*, PII) must have policies that provide guidance on the sharing and retention of such information.⁸²
- (A) PII gathered by one Federal agency should only be shared with another Federal, state, or local agency, or other organization when the following criteria are met:⁸³
 - (1) The information sharing is within the agency’s existing authorities;⁸⁴
 - (2) The sharing is appropriate and consistent with the routine uses listed in the applicable SORN(s), or conducted through an interagency agreement, *e.g.*, memorandum of understanding;⁸⁵
 - (3) The receiving agency or organization is authorized to receive the information and even then, only the minimal data (or data elements) should be shared to fulfill the authorized mission or business need;⁸⁶ and
 - (4) The receiving agency agrees to protect the information and retain it only as long as necessary; and to re-disseminate the information only in accordance with the criteria listed above.⁸⁷
 - (B) When PII is posted on a social media website or application, or sent to a Federal agency in connection with the transaction of public business, it may become a “federal record.” This requires that the agency:⁸⁸
 - (1) Maintain a copy of the appropriate records retention policies;⁸⁹
 - (2) Develop the appropriate record retention schedule(s) specifically to cover the information collected through social media that outline what information should be retained and for how long;⁹⁰ and

⁸⁰ CIO Council, Privacy Best Practices for Social Media, July 2013, at 9.

⁸¹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 9.

⁸² CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸³ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸⁴ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸⁵ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸⁶ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸⁷ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸⁸ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁸⁹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁹⁰ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

- (3) Ensure that the retention policies and schedules are clearly described in, and are consistent with, applicable PIAs and SORNs.⁹¹

13-5. Adapted PIA. The FCC must conduct an **Adapted PIA** when using a third-party website or application that makes PII available to the Commission.⁹²

- (A) The **Adapted PIA** must address the specific functions of the website or application by adapting or tailoring it to address the functions of the website or application with specific questions, as appropriate, in addition to generally following the Commission's existing PIA template's question format.⁹³
- (B) This adapted PIA's format will solicit and should describe the following information:⁹⁴
 - (1) The specific purposes for the FCC's use of this third-party website or application;⁹⁵
 - (2) Any PII that is likely to become available to the FCC through this public use of the third-party website or application;⁹⁶
 - (7) The FCC's intended or expected use(s) of the PII;⁹⁷
 - (8) With whom will the FCC share or transmit this PII, including entities and parties both inside and outside the FCC;⁹⁸
 - (9) Whether and how the FCC will maintain any PII, and for how long;⁹⁹
 - (10) How the FCC will secure the PII that it uses or maintains;¹⁰⁰
 - (11) What other privacy risks exist and how will the FCC will mitigate these risks;¹⁰¹ and
 - (12) Whether the FCC's activities will create a new or modify an existing system of records under the Privacy Act.¹⁰²

⁹¹ CIO Council, Privacy Best Practices for Social Media, July 2013, at 10.

⁹² OMB Memorandum M-10-22, June 25, 2010, at 4; OMB Circular A-130, at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/

⁹³ OMB Memorandum M-10-22, June 25, 2010, at 4; OMB Circular A-130, at http://www.whitehouse.gov/omb/Circulars_a130_a130trans4/

⁹⁴ OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010, at 4; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

⁹⁵ OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010, at 4; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

⁹⁶ OMB Memorandum M-10-22, at 4; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

⁹⁷ OMB Memorandum M-10-22, at 4; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

⁹⁸ OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

⁹⁹ OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

¹⁰⁰ OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

¹⁰¹ OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

¹⁰² OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

- Notes:** (1) **Appendix 6, Adapted Privacy Impact Assessment (PIA) Template;** and
(2) **Appendix 7, OMB Guidance on the Adapted (PIA) Template.**

13-6. Third-Party Websites and Applications. The FCC's use of third-party websites and applications requires that:¹⁰³

- (A) Each third-party website or application should be covered by an **adapted PIA**.¹⁰⁴
- (B) A single **adapted PIA** may cover multiple websites or applications that are functionally comparable, as long as the FCC's practices are substantially similar across each website and application,¹⁰⁵ which the **Privacy Threshold Analysis (PTA)**¹⁰⁶ will determine:
- (1) When a single adapted PIA may be used to cover the FCC's use of multiple social media websites where limited PII is made available to the agency but none is collected, shared, or maintained, as determined by the PTA;¹⁰⁷ or,
- (2) When the PTA determines that each website or an application may raise distinct privacy risks, which requires that a PIA must be conducted specifically to cover each website or application to ensure that the website's potential, distinct privacy risks are evaluated.¹⁰⁸
- (3) The FCC will display the FCC's official seal or logo and name in a prominent location on each individual third-party website and application so that anyone reviewing each individual webpage will be informed that it is an **official webpage** associated with an agency of the Federal Government.¹⁰⁹
- (4) If the FCC uses a third-party hosted social media website (*e.g.*, the FCC's Facebook page) that provides the FCC with links on the social media website to any non-government websites (*e.g.*, a non-profit organization's website), the FCC must ascertain whether the non-government website can display an affiliation to the FCC by posting its seal or name as an affiliated entity.¹¹⁰
- (5) The FCC will provide links to the relevant privacy policies of the third-party websites and applications that are being used (when feasible).¹¹¹

¹⁰³ OMB Memorandum M-10-23, at 5.

¹⁰⁴ OMB Memorandum M-10-23, at 5.

¹⁰⁵ OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

¹⁰⁶ CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 14.

¹⁰⁷ OMB Memorandum M-10-23, at 5; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

¹⁰⁸ OMB Memorandum M-10-23, at 6; OMB Memorandum for CIOs, Dec. 29, 2011, at 4.

¹⁰⁹ OMB Memorandum M-10-23, at 5.

¹¹⁰ OMB Memorandum M-10-23, at 5.

¹¹¹ OMB Memorandum M-10-23, at 5.

- (6) The FCC should establish and post an appropriate Privacy Policy or Privacy Notice on each social media website and/or application to inform users (when feasible) that:¹¹²

The FCC does not control or operate this social media website or application;¹¹³

- (7) The FCC will indicate if and how the it will maintain, use, or share PII provided on the social media website or application;¹¹⁴
- (8) The FCC will make clear that any PII provided on the social media website or application may be provided to the Commission;¹¹⁵ and
- (9) The FCC will provide a link or instructions on how to reach the FCC’s official website at: www.fcc.gov.¹¹⁶
- (C) The Commission will contact OMB, when advisable, to provide guidance to the Commission on the PIA process and to suggest model PIAs and other resources that may be useful.¹¹⁷
- (D) The Commission will conduct periodic reviews of these third party websites and applications to ensure that the information in the adapted PIA is still current, applicable, and in compliance with its policies and programs.¹¹⁸
- (E) The Commission will re-visit these websites and/or applications to update the PIA should there be changes that create new or different privacy impacts and risks.¹¹⁹
- (F) The FCC may allow comments, viewpoints, and opinions on its social media websites or applications (regardless of whether the sites/applications are agency or third-party hosted), but the FCC must respect the public’s First Amendment rights.¹²⁰
- (G) The FCC will monitor the website and will remove any public comments that are political or endorse a political candidate, target specific individuals or groups, are abusive, contain sensitive PII, or are similarly unacceptable.¹²¹

¹¹² OMB Memorandum M-10-23, at 5.

¹¹³ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 8.

¹¹⁴ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 8.

¹¹⁵ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 8.

¹¹⁶ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 8.

¹¹⁷ OMB Memorandum M-10-23, at 5.

¹¹⁸ OMB Memorandum M-10-23, at 5; CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 5.

¹¹⁹ OMB Memorandum M-10-23, at 5; CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 5.

¹²⁰ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 9.

¹²¹ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 9.

- (H) The FCC’s policy concerning monitoring comment and removing (inappropriate) comments should be noted in the Privacy Notice. The FCC should also be prepared to respond to any public reaction when comments are deleted.¹²²
- (I) The FCC will display a **disclaimer** or **policy statement** that indicates that third party comments do not reflect the views of the FCC.¹²³
- (J) The FCC will develop operational use policies and procedures that are approved and documented by senior agency leadership (*e.g.*, Commissioners, SAOP, CIO, CSIO, and OGC) to cover operational uses due to their sensitivity and that include regular, routine reviews to ensure privacy and program compliance.¹²⁴

13-7. Privacy Policy. The FCC will publish its privacy policy on its website in accordance with OMB guidelines for third-party websites and applications.¹²⁵

- (A) The Commission’s privacy policy will describe how it uses third-party websites and applications:¹²⁶
 - (1) The specific purpose(s) of the FCC’s use(s) of third-party websites or applications;¹²⁷
 - (2) How the FCC will use the PII that becomes available through the use of the third-party websites or applications;¹²⁸
 - (3) Who at the FCC will have access to the PII;¹²⁹
 - (4) With whom the PII will be shared outside the FCC;¹³⁰
 - (5) Whether and how the FCC will maintain the PII, and for who long;¹³¹
 - (6) How the FCC will secure the PII that it uses or maintains;¹³² and
 - (7) What other privacy risks exist and how will the FCC mitigate those risks.¹³³
- (C) The privacy policy should, when feasible, provide links to the privacy policy of the third-parties websites and applications that are being used.¹³⁴

¹²² CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 11.

¹²³ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 9.

¹²⁴ CIO Council, Privacy Best Practices for Social Media, July 2013, at 6.

¹²⁵ OMB Memorandum M-10-23, at 5; OMB Memorandum M-99-18; OMB Memorandum M-03-22.

¹²⁶ OMB Memorandum M-10-23, at 5.

¹²⁷ OMB Memorandum M-10-23, at 5.

¹²⁸ OMB Memorandum M-10-23, at 5.

¹²⁹ OMB Memorandum M-10-23, at 5.

¹³⁰ OMB Memorandum M-10-23, at 5.

¹³¹ OMB Memorandum M-10-23, at 5.

¹³² OMB Memorandum M-10-23, at 5.

¹³³ OMB Memorandum M-10-23, at 6.

¹³⁴ OMB Memorandum M-10-23, at 6.

13-8. Privacy Act Notices. The FCC should, when feasible, post a **Privacy Act Notice** on third-party websites and/or applications that the Commission uses. (The requirement is similar to the **Privacy Act Statement** that is required for a FCC form or other Commission documents that request PII.)

(A) The **Privacy Act Notice** will:

- (1) Explain that the website or application is not a government website or application, that it is controlled or operated by a third party, and that the FCC's privacy policy does not apply to the third party;¹³⁵
- (1) Indicate whether and how the FCC will maintain, use, or share PII that becomes available through the use of the third-party website or application;¹³⁶
- (2) Explain that by using the website or application to communicate with the FCC, individuals may be providing nongovernment third-parties with access to their PII;¹³⁷
- (3) Direct individuals to the FCC's official website;¹³⁸ and
- (4) Direct individuals to the FCC's privacy policy.¹³⁹

(B) The FCC's **Privacy Act Notice** must be conspicuous, salient, labeled clearly, uses plain English, and is prominently displayed at all locations where visitors to the FCC website may make their PII available to the Commission.¹⁴⁰

(D) On the main page of the social media website or application and the social media Privacy Policy or Notice, the FCC should place a clear and conspicuous link to the Commission's Privacy Policy that is found on its official website.¹⁴¹

13-9. Universal Resource Locator (URL) Shortening Technology. Federal agencies should weigh the risks before implementing any URL shortening technology on public or third-party websites, in e-mails, or in other electronic communications.

(A) If the FCC employs or redirects individuals to a third party website that uses URL shortening technologies, the Commission must provide clear and prominent notice to the individuals before directing them to that website.¹⁴²

¹³⁵ OMB Memorandum M-10-23, at 6.

¹³⁶ OMB Memorandum M-10-23, at 6.

¹³⁷ OMB Memorandum M-10-23, at 6.

¹³⁸ OMB Memorandum M-10-23, at 6.

¹³⁹ OMB Memorandum M-10-23, at 6.

¹⁴⁰ OMB Memorandum M-10-23, at 6.

¹⁴¹ CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 8.

¹⁴² CIO Council Recommendations, "Privacy Best Practices for Social Media," July 2013, at 12.

- (B) The notice can be included in an “exit” page, “pop-up,” or in an electronic communication to the individual.¹⁴³
 - (C) The third party website must have clear and prominent notice on its website advising of the use of this technology.¹⁴⁴
- 13-10. SAOP Guidance. The SAOP is responsible for determining the suitability of using third-party websites and applications:¹⁴⁵
- (A) The SAOP is to have a “central policy-making role” with “overall responsibility and accountability for ensuring that the agency’s implementation of information privacy protections.”¹⁴⁶
 - (B) OMB guidelines also direct agencies to confer with their SAOP at the earliest possible stage of the planning process, and to consult with the SAOP through implementation and post-implementation review of any third-party website and application usage.¹⁴⁷
 - (C) The SAOP will supervise and provide guidance on the adapted PIA:¹⁴⁸
 - (1) To determine how many PIAs are needed;¹⁴⁹
 - (2) To identify when updates to PIAs are needed;¹⁵⁰ and
 - (3) To insure full compliance with OMB policies.¹⁵¹
- 13-11. OMB Assistance. The OMB desk officer should be consulted at privacy-oira@omb.eop.gov for clarification and guidance when additional assistance is needed to determine the appropriateness and suitability for using these third-party websites and applications.¹⁵²

¹⁴³ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 12.

¹⁴⁴ CIO Council Recommendations, “Privacy Best Practices for Social Media,” July 2013, at 12.

¹⁴⁵ OMB Memorandum M-10-23, at 6.

¹⁴⁶ OMB Memorandum M-10-23, at 6.

¹⁴⁷ OMB Memorandum M-10-23, at 6.

¹⁴⁸ OMB Memorandum M-10-23, at 5.

¹⁴⁹ OMB Memorandum M-10-23, at 5.

¹⁵⁰ OMB Memorandum M-10-23, at 5.

¹⁵¹ OMB Memorandum M-10-23, at 5.

¹⁵² OMB Memorandum M-10-23, at 7.

CHAPTER 14

PRIVACY TRAINING

- 14-1. Privacy Training Policy. Because of the capability of information technology to capture and disseminate information in an instant, all FCC employees and contractors must remain mindful of privacy and their obligation to protect PII. The FCC has a duty to inform and educate employees and contractors of their responsibility for protecting PII.¹
- 14-2 Privacy Training Requirements. Since 2006, the FCC has required privacy training for all Commission employees and contractors.² Privacy training is an official FCC policy and is conducted under the guidance of the SAOP, CIO, and OGC.
- (A) All new Commission employees and appropriate Commission contractors are required to take an **initial privacy training program** when they are hired by the FCC or begin work at the FCC through their contract employer.³
- (1) The goal of the initial training is to familiarize employees and contractors with their privacy responsibilities, including Federal privacy laws, regulations, and policies, and the ramifications of inappropriate access and disclosure of PII, *i.e.*, “data breach,” before permitting them access to the Commission’s information systems and the information that these systems contain, especially the PII.⁴
- (2) The initial formal training is supplemented by a 2-page fact sheet/newsletter entitled “Personally Identifiable Information,” which provides employees and contractors with a document that they can print and used as a reference tool to enable them to identify and protect PII in the course of their job duties and responsibilities. The New Employee Orientation package contains a copy of this “Personally Identifiable Information” fact sheet/newsletter.⁵
- (3) Further, employees and contractors are required to take, complete and pass the Security Awareness training. This electronic, mandatory course includes a comprehensive section on Privacy Act regulations, rules and PII protections in the federal government and, specific information of FCC Privacy and PII protection practices and procedures. It also contains specific examples of FCC protected PII systems and documents.
- (B) All Commission employees (including managers) and appropriate Commission contractors are required to take an **annual privacy refresher training** as noted in (A)(3) above.

¹ OMB Memorandum M-03-22, Attachment A, at 10. Also cite A-108, Section 12 g. A-130, Appendix III, Appendix J of NIST SP-800-53, & Directive 1479.5 Cyber Security Policy (appropriate sections on Privacy & Security awareness training)

² FCC Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” September 22, 2007, at 8.

³ FCC Memorandum, Sept. 22, 2007, at 8.

⁴ FCC Memorandum, Sept. 22, 2007, at 15.

⁵ FCC Memorandum, Sept. 22, 2007, at 8.

- (1) The refresher training provides additional instruction to employees and contractors to ensure that they continue to understand their responsibilities to protect PII.
- (2) This annual course also contains additional questions on the duties and responsibilities for safeguarding privacy for supervisors and managers.
- (C) The Commission requires system managers to provide additional, **specialize privacy training** for their employees and contractors, such as telecommuters, HRM staff, IT staff, etc., who have access to the PII in the information systems, databases, and paper document files that they use or to which they may have access as part of their job duties.⁶
- (D) The Commission also provides more **specialized or advanced privacy training**.
 - (1) The advanced or specialized training is designed for supervisors, employees, and contractors whose job duties and responsibilities require their “interaction” with PII, such as system managers and employees who have access to documents and files containing PII and/or employees and contractors who maintain the FCC’s computer network databases.
 - (2) Advanced or specialized training is also given to employees and contractors when they are assigned new or expanded duties that increase their access to and/or responsibilities for PII in the Commissions information systems and the PII that these systems collect, use, and store.
- (F) In all the Commission’s training courses, including the initial, refresher, and advanced or specialized training, there is instruction on the acceptable rules of behavior and the consequences when the rules are not followed. Training also includes a description of privacy and security responsibilities as they pertain to participants in the FCC’s telework program.⁷
- (G) In B/Os where supervisors, employees, and contractors interact with PII on a regular basis and require advanced or specialized training, the system manager is advised as part of the PIA review that it is incumbent upon them to make their employees and contractors aware of the need for precautions to prevent any unintended disclosure of PII during the course.
- (H) All the Commission’s privacy training courses, including initial, annual refresher, and specialized training, require that the individual pass a quiz to receive FCC University credit for each course.

14-3. Cyber Security. Employees and contractors actors are required to take security awareness training.

⁶ FCC Memorandum, Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” September 22, 2007, at 8.

⁷ OPM, Memorandum for Chief Human Capital Officers, *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft*, June 18, 2007; FCC Telework Request Form and Agreement; FCC Memorandum, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” September 22, 2007, at 15.

- (A) Cyber Security Training includes information on privacy issues as these relate to various cyber security issues, such as viruses and malware; and acceptable rules of behavior such as never disclosing very sensitive information like SSNs, passport and visa numbers, credit card numbers in e-mails or on the Internet. As noted in 14-2 (A)(3) above, it contains a comprehensive, FCC specific section on Privacy and PII protection.
 - (B) The FCC's *Cyber Security Policy Directive* FCCINST 1479.5 (May, 2015) conforms to DHS's *Directive 4300* (considered the "gold standard"). This FCC Directive includes the latest Federal privacy and cyber security laws, regulations, policies and practices.
- 14-4 Sensitive Information. The Commission also offers ten job-specific IT Security courses for various employees and contractors. These courses include mention of the need to limit and control access to information systems that contain various types of sensitive information, including information that is protected by the Privacy Act, *e.g.*, PII.⁸

⁸ FCC Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," September 22, 2007, at 8.

CHAPTER 15

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) PRIVACY REQUIREMENTS

- 15-1. Policy. The Federal Information Security Modernization Act (FISMA) of 2014 has established information security priorities and reporting requirements for Federal agencies.¹
- (A) FISMA was enacted to protect Federal resources by providing a comprehensive framework for supporting the effectively of information security controls, including protections for PII.²
 - (B) Federal agencies are responsible for managing the security of their information and information systems, including those that collect, store, use, maintain, and dispose of PII, through a variety of risk-based security controls and initiatives.³
 - (C) FISMA requires Federal agencies to submit an annual report to OMB on their privacy programs and their compliance with Federal statutes and OMB regulations.⁴
 - (D) These guidelines are intended to explain what FISMA is and how Federal agencies must comply with these requirements, as established by OMB.⁵
- 15-2. Reporting Requirements. The Office of Management and Budget (OMB) has established these annual FISMA reporting requirements for all Federal agencies:
- (A) All Federal agencies will submit their annual fiscal year FISMA metrics via Cyberscope to the Department of Homeland Security, usually in November of each fiscal year.⁶
 - (B) Following OMB review, all agency FISMA reports are then submitted to Congress.⁷
- Note:** (1) **Appendix 8, SAOP Privacy Annual FISMA Privacy Report**, and
- (2) **Appendix 9, Bureau, Office, and OMD Division FISMA Privacy Activities Reporting Questionnaire** are the two forms that the SAOP has instructed the Privacy Manager to use for the Commission's annual B/O/Ds FISMA reviews.

¹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at 1.

² OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, October 3, 2014, at 1.

³ OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, October 3, 2014, at 2.

⁴ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at 1.

⁵ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at 1.

⁶ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

⁷ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

15-3. Agency Letter. The FCC's annual FISMA report to OMB should include official cover letter signed by the head of the FCC (or his/her designate) and provide the FCC's comprehensive assessment of the adequacy and effectiveness of the Commission's information security/privacy policies, procedures, and practices. This letter must include the following details, as specified in 44 U.S.C. 3554:⁸

- (A) A description of each major incident including:⁹
 - (1) Threats and threat actors, vulnerabilities, and impacts;¹⁰
 - (2) Risk assessments conducted on the system before the incident;¹¹
 - (3) The status of compliance with the affected information system with security requirements at the time of the incident;¹² and
 - (4) The detection, response, and remediation actions the Commission has completed.¹³
- (B) For each major incident that involved a breach of PII, the description must also include:¹⁴
 - (1) The number of individuals whose information was affected by the major incident;¹⁵ and
 - (2) A description of the information that was breached or exposed.¹⁶
- (C) The total number of cyber threats, including a description of system impact levels, types of incident, and locations of affected systems:¹⁷

⁸ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

⁹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹⁰ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹¹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹² OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹³ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹⁴ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹⁵ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹⁶ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹⁷ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

- (D) Progress towards meeting the annual FY FISMA Metrics: agency-specific metrics data demonstrating the Commission's progress towards meeting the FY FISMA metrics established by OMB, DHS, and the CIO Council.¹⁸
- (E) Progress toward meeting the Cybersecurity CAP goal: agency-specific review of the Commission's performance with regard to the Administration's cybersecurity priorities with their Performance Improvement Officer and inclusion of data pertaining to the cybersecurity performance metrics.¹⁹

15-2. SAOP Section Report Metrics:²⁰

Section I: Information Security Systems for agency and contractor systems:²¹

- 1(a) Number of Federal systems that contain personal information in an identifiable form;
- 1(b) Number of systems in 1(a) for which a Privacy Impact Assessment (PIA) is required under the E-Government Act;
- 1(c) Number of systems in 1(b) covered by a current PIA;
- 1(d) Number of systems in 1(a) for which a System of Records Notice (SORN) is required under the Privacy Act; and
- 1(e) Number of systems in 1(d) for which a current SORN has been published in the *Federal Register*.

Section 2: PIAs and SORNs:²²

- 2(a) Provide the URL of the centrally located page on the organization web site that provides working links to organization PIAs; and
- 2(b) Provide the URL of the centrally located page on the organization web site that provides working links to the published SORNs.

Section 3: SAOP Responsibilities:²³

- 3(a) Can your organization demonstrate with documentation that the SAOP participated in all organization information privacy compliance activities?

¹⁸ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

¹⁹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

²⁰ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I; OMB Memorandum M-15-

²¹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

²² OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

²³ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

- 3(b) Can your organization demonstrate with documentation that the SAOP participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals, as well as testimony and comments under OMB Circular A-19?
- 3(c) Can your organization demonstrate with documentation that the SAOP participates in assessing the impact of the organization's use of technology on privacy and the protection of personal information?

Section 4: Privacy Training:²⁴

- 4(a) Does your organization have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations, and policies, and understand the ramification of inappropriate access and disclosure?
- 4(b) Does your organization have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) that handle personal information, that are directly involved in the administration of personal information or information technology systems, or that have significant security responsibilities?

Section 5: PIA and Web Privacy Policies and Processes:²⁵ Does the organization have a written policy or process for each of the following:

- 5(a) PIA Practices:
 - 5(a)(1) Determining whether a PIA is needed;
- 5(b) Web Privacy Practices:
 - 5(a)(2) Conducting a PIA;
 - 5(a)(3) Evaluating changes in technology or business practices that are identified during the PIA process;
 - 5(a)(4) Ensuring system owners, privacy officials, and IT experts participate in conducting the PIA;
 - 5(a)(5) Making PIAs available to the public as required by law and OMB policy;
 - 5(a)(6) Monitoring the organization's systems and practices to determine when and how PIAs should be updated;

²⁴ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

²⁵ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

5(a)(7) Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained;

5(b)(1) Determining the circumstances where the organization's web-based activities warrant additional consideration of privacy implications;

5(b)(2) Making appropriate updates and ensuring continued compliance with stated web privacy policies;

5(b)(3) Requiring machine-readability of public-facing organization web sites (*i.e.*, use of P3P);

Section 6: Conduct of Mandated Reviews:²⁶ Did your organization perform the following reviews as required by the *Privacy Act of 1974*, the *E-Government Act of 2002*, and the *Federal Agency Data Mining Reporting Act of 2007*?

6(a) Section (m) Contracts;

6(b) Records Practices;

6(c) Routine Uses;

6(d) Exemptions;

6(e) Matching Programs;

6(f) Training;

6(g) Violations: Civil Action;

6(h) Violations: Remedial Action;

6(i) System of Records Notices;

6(j) (e)(3) Statement;

6(k) Privacy Impact Assessments and Updates; and

6(l) Data Mining Impact Assessment.

Section 7: Written Privacy Complaints:²⁷ Indicate the number of written complaints for each type of privacy issue received by the SAOP or others at the organization.

7(a) Process and Procedural – consent, collection, and appropriate notice;

²⁶ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

²⁷ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

- 7(b) Redress – non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters;
- 7(c) Operational – inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction; and
- 7(d) Referrals – complaints referred to another organization with jurisdiction.

Section 8: Policy Compliance Review.²⁸

- 8(a) Does the organization have current documentation demonstrating review of the organization’s compliance with information privacy laws, regulations, and policies;
- 8(b) Can the organization provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews;
- 8(c) Does the organization use technologies that enable continuous auditing of compliance with stated privacy policies and practices; and
- 8(d) Does the organization coordinate with the organization’s Inspector General on privacy program oversight.

Section 9: SAOP Advice and Guidance.²⁹ Has the SAOP provided formal written advice or guidance in each of the listed categories, and briefly describe the advice or guidance if applicable:

- 9(a) Organization policies, orders, directives, or guidance governing the organization’s handling of personally identifiable information;
- 9(b) Written agreements (either interagency or with non-Federal entities) pertaining to information sharing, computer matching, and similar issues;
- 9(c) The organization’s practices for conducting, preparing, and releasing SORNs, and PIAs;
- 9(d) Reviews or feedback outside of the SORN and PIA process (*e.g.*, formal written advice in the context of budgetary or programmatic activities or planning); and
- 9(e) Privacy training (either stand-alone or included with training on related issues).

Section 10: Agency Use of Web Measurement and Customization Technologies.³⁰

²⁸ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

²⁹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁰ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

- 10(a) Does the organization use web management and customization technologies on any web site or application;
- 10(b) Does the organization annually review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance;
- 10(c) Can the organization demonstrate, with documentation, the continued justification for, and approval to use, web management, and customization technologies;
- 10(d) Can the organization provide the notice language or citation for the web privacy policy that informs visitors about the use of web management and customization technologies; and
- 10(e) Number of requests for Tier 3 web measurement and customization technologies approved by the SAOP during the reporting period (see OMB M-10-22 for more information).

Section 11: Information System Security.³¹

- 11(a) Number of authorizations to operate (ATOs) or reauthorizations issued during the reporting period; and
- 11(b) Number of ATOs or reauthorizations approved by the SAOP during the reporting period (OMB M-14-04 provided that SAOP approval is required as a precondition for the issuance of an ATO).

Section 12: Breach Response and Notification:³² Pursuant to FISMA, each Federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems. New US-CERT Federal Incident Notification Guidelines are effective October 1, 2014:

- 12(a) Number of confirmed breaches reported by your organization to the U.S. Computer Emergency Readiness Team (US-CERT) during the reporting period;
- 12(b) Number of confirmed non-cyber related (*e.g.*, paper) breaches experienced by your organization during the reporting period (OMB M-15-01 provided that non-cyber related incidents should be reported to your agency's privacy officer and not to US-CERT);
- 12(c) Number of persons potentially affected by all confirmed breaches, both cyber and non-cyber, during the reporting period (approximate figures if precise figures are not available); and

³¹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³² OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

- 12(d) Number of potentially affected persons who were provided notification about a breach of information experienced by your organization that occurred during the reporting period.

15-3. Addenda:

- (1) A document describing the FCC's privacy training for employees and contractors;³³
- (2) A copy of the FCC's Breach Notification Policy;³⁴
- (C) A document updating the description of the FCC's progress on reducing the holdings of personally identifiable information (PII), including elimination of unnecessary use(s) of Social Security numbers;³⁵ and
- (D) A memorandum describing the FCC's privacy program, including the role of the Senior Agency Official for Privacy (SAOP) and the resources that the Commission has dedicated to privacy-related functions.³⁶

Note: For the purposes of this reporting requirement, privacy-related functions include, but are not limited to, complying with all laws, regulations, and policies relating to privacy, as well as applying the appropriate privacy standards and other best practices.³⁷

- (E) As assessment of whether the SAOP has the necessary authority, independence, access to agency leadership, subject matter expertise, and resources to effectively manage and oversee all privacy-related functions across the Commission;³⁸ and
- (F) Any other information that OMB should know about how privacy-related functions are performed at the FCC.³⁹

Note: OMB requires agencies to submit these documents whether or not the documents have changed from versions submitted in previous years.⁴⁰

³³ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁴ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁵ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁶ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁷ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁸ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

³⁹ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

⁴⁰ OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, October 30, 2015, at Section I.

CHAPTER 16

FCC PRIVACY BREACH NOTIFICATION POLICY

- 16-1. **Purpose.** This Chapter sets forth the FCC's policy to plan, prepare for, and respond to a suspected or confirmed breach of personally identifiable information (PII).
- (A) This Chapter reflects changes to laws, policies, and best practices that have emerged since OMB first required agencies to develop plans to respond to a **Data Breach**.¹
 - (B) Guidance is provided on the steps the FCC will take to evaluate the risk of harm to individuals potentially affected by a data breach and, where appropriate, to provide potentially affected individuals with guidance and services to help mitigate the risk.²
 - (1) This guidance provides consistency in the way that Federal agencies are to respond to a breach by requiring common standards and processes.³
 - (2) This guidance also provides flexibility in the way to tailor the Commission's response based upon the specific facts and circumstances of each breach and an analysis of the risk of harm to potentially affected individuals.⁴
- Note:** OMB's guidance allows Federal agencies to impose stricter standards that are consistent with their missions, authorities, circumstances, and identified risks.⁵
- (C) This guidance applies to all FCC information and information systems as defined by OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016. This guidance does not apply to National Security Systems (under 44 U.S.C. 3554) in conducting Commission business. See *FCC Directive 1133.1 FCC Insider Threat Program*.
- 16-2. **Definitions.** For purposes of this chapter the following definitions and terms shall apply:
- (A) **Personally Identifiable Information (PII)**, as defined in OMB Circular No. A-130, and elsewhere in this *Directive*, refers to 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.⁶
 - (1) There are many different types of information that can be used to distinguish or trace an individual's identity such as his/her name, social security number, biometric records, etc., or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and

¹ OMB Memorandum M-17-12, Jan. 3, 2017, *Preparing for and Responding to a Breach of Personally Identifiable Information*, at 1.

² OMB Memorandum M-17-12, at 1.

³ OMB Memorandum M-17-12, at 1.

⁴ OMB Memorandum M-17-12, at 1.

⁵ OMB Memorandum M-17-12, at 2.

⁶ OMB Memorandum M-17-12, at 8.

place of birth, mother's maiden name, etc.; and therefore, the term PII is necessarily broad.⁷

- (2) To determine whether information is PII, the Commission performs an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual.⁸
- (3) These assessments are made through **Privacy Threshold Assessments (PTAs)** and **Privacy Impact Assessments (PIA)** on all FCC information systems.

Note: Chapters 2, 3 and 9 provide information about these administrative requirements.

- (4) The Commission also recognizes, in performing these assessments, that information that is not PII can become PII whenever additional information becomes available in **any medium** or from **any source** that would make it possible to identify an individual.⁹

(B) An **Incident** is an occurrence that:¹⁰

- (1) Actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of Information or an Information System; or
- (2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (3) Is the result from one or more of these unauthorized actions to information or an information system:
 - (1) **Unauthorized modification** – the act or process of changing components of information and/or information systems;¹¹
 - (2) **Unauthorized deletion** – the act or process of removing information from an information system;¹²
 - (3) **Unauthorized exfiltration** – the act or process of obtaining, without authorization or in excess of authorized access, information from an information system without modifying or deleting it;¹³ and/or
 - (4) **Unauthorized access** – the act or process of logical or physical access without permission to a Federal agency information, information system, application, or resource.¹⁴

⁷ OMB Memorandum M-17-12, at 8.

⁸ OMB Memorandum M-17-12, at 8.

⁹ OMB Memorandum M-17-12, at 8.

¹⁰ 44 U.S.C. § 3552(b)(2); OMB Memorandum M-17-12, at 8.

¹¹ OMB Memorandum M-17-05, at 8.

¹² OMB Memorandum M-17-05, at 8.

¹³ OMB Memorandum M-17-05, at 8.

¹⁴ OMB Memorandum M-17-05, at 8.

(C) A **Breach** is a type of incident.¹⁵

- (1) A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence(s) where:¹⁶
 - (a) A person other than an authorized user accesses or potentially accesses personally identifiable information (PII), or
 - (b) A person accesses personally identifiable information (PII) for other than authorized purpose.¹⁷
- (2) A breach is not limited to a network intrusion, targeted attack that exploits website vulnerabilities, or an attack executed via email message or attachment.
- (3) A breach may also include the loss or theft of physical documents and portable electronic storage media, or an oral disclosure of PII to a person who is not authorized to receive that information.
- (4) An occurrence may sometimes be first identified as an incident, but later identified as a breach once it is determined to involve PII.¹⁸
- (5) Common examples of a breach situation that may involve the FCC include:¹⁹
 - A laptop or portable storage device storing PII is lost or stolen.
 - An email containing PII is inadvertently sent to and received by the wrong person.
 - A folder containing PII is stored on a shared drive without appropriate access controls.
 - A box of documents with PII is lost during shipping.
 - An unauthorized third party overhears FCC employees discussing PII about an individual seeking employment or Federal benefits.
 - An IT system that maintains PII is accessed and compromised by a malicious actor.
 - An employee inadvertently posts PII on a public website or on a site internal to the FCC.²⁰

(D) A breach constitutes a **Major Incident** when the incident involves PII that, if exfiltrated, modified, deleted, or otherwise compromised:

¹⁵ OMB Memorandum M-17-12, at 9.

¹⁶ OMB Memorandum M-17-12, at 9.

¹⁷ OMB Memorandum M-17-12, at 9.

¹⁸ OMB Memorandum M-17-12, at 9.

¹⁹ OMB Memorandum M-17-12, at 9.

²⁰ OMB Memorandum M-17-12, at 9 - 10.

- (1) Is likely to result in a demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.²¹
- (2) Involves an unauthorized modification of, unauthorized deletion of, authorized exfiltration of, or unauthorized access to the PII of 100,000 or more individuals.²²
- (3) Must also be considered a **significant cyber incident** under *Presidential Policy Directive-41* (PPD-41).²³

Note: Only when a breach of PII that constitutes a “major incident” is the result of a **cyber incident** will it meet the definition of a “significant cyber incident” and trigger the coordination mechanisms outlined in *Presidential Policy Directive-41* (PPD-41).²⁴

- (E) **Federal Information** means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.²⁵
- (F) **Federal Information System** means an information system used or operated by the FCC, a FCC contractor, or by another organization on behalf of the FCC.²⁶
- (G) **High Value Asset** is an information system which collects, stores, maintains, uses, and disposes of (when no longer necessary) a collection of records of special importance in the aggregate for the Commission.²⁷
- (H) **Chief Information Officer (CIO)** is the FCC’s senior agency official in charge of and responsible for all information collections and uses at the FCC. The CIO is the contact point for employee notifications about breaches of paper-based PII.
- (I) **Chief Information Security Officer (CISO)** is the FCC’s senior agency official in charge of and responsible for providing oversight on all aspects of cybersecurity at the FCC. The CISO is the contact point for FCC-related notifications of breaches of computer-based PII.
- (J) **Chief Security Officer (CSO)** in the **Security Operations Center (SOC)** is the FCC’s senior agency official providing oversight on all aspects of the Commission’s physical security program, including guard staff and access controls, to ensure that FCC facilities and employees, at headquarters in Washington DC, Gettysburg PA, and field offices, are protected from potentially disorderly or destructive individuals, theft of government and

²¹ OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, at 7.

²² OMB Memorandum M-17-05, at 8.

²³ OMB Memorandum M-17-05, at 8.

²⁴ OMB Memorandum M-17-05, at 8.

²⁵ OMB Memorandum M-17-12, at 47.

²⁶ OMB Memorandum M-17-12, at 47.

²⁷ OMB Memorandum M-16-03, at 7.

personal property, and civil emergencies. The SOC is the contact point for employee notifications about breaches of paper-based PII.

- (K) **Chief Human Capital Officer (CHCO)** assists when employee misconduct results in a Breach or when an employee is suspected of intentionally causing a breach or violating Commission policy;
- (L) **Office of Inspector General (OIG)** assists when a breach involves the violation of a law or when a Breach is a subject of a law enforcement investigation in coordination with the CSO.
- (M) **FCC Information System Owners** provide critical knowledge concerning information and the information system to assist the Breach Response Team (BRT) with assessing the parameters of the data breach;
- (N) **FCC Managing Director (MD)** has the overall responsibility for the implementation of an agency-wide information security and privacy program as required by the laws and regulation as directed by the FCC for ensuring compliance with all government-wide legal and policy requirements.
- (O) **Deputy Chief Information Security Officer for Resiliency (DCIOR)** is responsible for all information systems and their security as well as for ensuring FISMA compliance.
- (P) **Privacy Manager (PM)** coordinates the Commission's Privacy Act program including processing requests under the Privacy Act, serving as liaison to OMB and Congress in establishment of new or revised systems of records and notices (SORNs) and any exemptions under the Privacy Act, responding to internal, external, and public inquiries concerning the Commission's system of records, generating all Privacy Threshold Analyses (PTAs) and Privacy Impact Analyses (PIAs) and reporting to OMB under the Privacy portion of the annual FISMA filing.
- (Q) **Chief Security Officer (CSO) in the Security Operations Center (SOC)** administers the physical security program to ensure that FCC facilities and employees, at headquarters in Washington DC, Gettysburg PA, and field offices, are protected from potentially disorderly or destructive individuals, theft of government and personal property, and civil emergencies. The CSO is the point of contact for FCC-related notifications involving breaches of paper-based PII.
- (R) **Network Security Operations Center (NSOC)** is the FCC organization that works with the Security Operations Center to maintain situational awareness of and visibility into the security posture of FCC information systems and networks. At the direction of the CISO, the NSOC is part of the Breach Response Team (BRT) that addresses any PII incident response, including reporting cybersecurity (computer-related) incidents to US-CERT, in accordance with this document.
- (S) **US Computer Emergency Readiness Team (US-CERT)** in the Department of Homeland Security (DHS) that coordinates the protection of federal civilian agencies information systems and networks against cyber-attacks. US-CERT is the organization to which all potential or confirmed breaches (whether in paper or electronic format) of PII must be reported.

- 16-3. Role of the Senior Agency Official for Privacy (SAOP). The SAOP is the FCC Chairman's designee who is responsible for ensuring compliance with applicable privacy requirements, including the responsibility to insure that there is adequate preparation for and an appropriate response to any information breach at the FCC. The SAOP's responsibilities are:
- (A) To ensure that all FCC SORNs include routine uses (and all other administrative requirements) that pertain to the disclosure of information necessary to respond to a breach either of the agency's PII or, as appropriate, to assist another agency in its response to a breach.²⁸
 - (B) To provide training and awareness for employees and contractors on how to report and respond to a Breach;²⁹
 - (C) To develop, implement, direct, and coordinate the FCC's formal breach management policies and procedures, including its **Breach Response Plan (BRP)** and the **Breach Response Team (BRT)** members;³⁰
 - (D) To maintain the appropriate breach response capabilities, including:
 - (1) Developing the appropriate criteria for convening the BRT as outlined in the FCC's BRP;³¹
 - (2) Creating a mechanism for notifying potentially affected individuals;³²
 - (E) To conduct and document an assessment of the risk of harm to individuals potentially affected by a breach, including factors to be considered when assessing these risks:³³
 - (1) Determining the number of employees and contractors with access to the PII;
 - (2) Determining whether the PII can be accessed on a regular basis from outside the FCC;
 - (3) Determining if any information is sent to individuals or entities outside the FCC (matching activities);
 - (4) Determining the appropriate measures to mitigate the identified risks depending upon the breach circumstances;³⁴
 - (5) Advising the FCC Chairman on whether to take any specific countermeasures, as appropriate;³⁵ and

²⁸ OMB Memorandum M-17-12, at 10-11.

²⁹ OMB Memorandum M-17-12, at 11.

³⁰ OMB Memorandum M-17-12, at 16.

³¹ OMB Memorandum M-17-12, at 16 - 17.

³² OMB Memorandum M-17-12, at 16.

³³ OMB Memorandum M-17-12, at 16.

³⁴ OMB Memorandum M-17-12, at 27.

³⁵ OMB Memorandum M-17-12, at 27.

- (6) Offering guidance and/or providing services, when appropriate to individuals potentially affected by the breach.³⁶

Note: Countermeasures and mitigation recommendations are detailed in Section 16-23.

16-5. Data Breach Response Plan. OMB guidelines require each Federal agency to develop and implement a **Breach Response Plan (BRP)**.

- (A) The BRP is a formal document that is tailored to the FCC's needs and specifically addresses its mission, size, structure, functions, and requirements.³⁷
- (B) The BRP details the FCC's policies and procedures for reporting, investigating, and managing a data breach at the FCC. At a minimum, it is to include the following elements:³⁸
- (1) **Breach Response Team (BRT)** that includes the specific agency officials who are chosen for their respective roles and responsibilities when responding to a breach.³⁹
 - (2) **Identification of Applicable Privacy Compliance Documentation** that includes the responsibility to identify any applicable Privacy Act system of records notices (SORNs), privacy impact assessments (PIAs), and privacy notices that may apply to the potentially compromised information.⁴⁰
 - (3) **Information Sharing to Respond to a Breach** that includes the potential information sharing within the agency, between agencies, or with a non-Federal entity that may arise following a breach:
 - To reconcile or eliminate duplicate records,
 - To identify potentially affected individuals, and/or
 - To obtain contact information to notify potentially affected individuals.⁴¹
 - (4) **Reporting Requirements** include the specific FCC Breach Response Team officials who are responsible for reporting a breach to US-CERT, law enforcement and oversight entities, and Congress, when appropriate.⁴²
 - (5) **Assessment of the Risk of Harm to Individuals Potentially Affected by a Breach** includes the factors the FCC should consider when assessing the risk of harm to potentially affected individuals.⁴³

³⁶ OMB Memorandum M-17-12, at 27.

³⁷ OMB Memorandum M-17-12, at 15 and 47.

³⁸ OMB Memorandum M-17-12, at 15.

³⁹ OMB Memorandum M-17-12, at 16.

⁴⁰ OMB Memorandum M-17-12, at 16.

⁴¹ OMB Memorandum M-17-12, at 16.

⁴² OMB Memorandum M-17-12, at 16.

⁴³ OMB Memorandum M-17-12, at 16.

- (6) **Mitigation of the Risk of Harm to Individuals Potentially Affected by a Breach** includes whether an FCC should provide guidance to potentially affected individuals, purchase identity theft services for potentially affected individuals, and/or offer methods for acquiring such services.⁴⁴
- (7) **Notification to Individuals Potentially Affected by a Breach** includes if, when, and how to provide notification to potentially affected individuals and other relevant entities.⁴⁵

Note: The analysis for reporting a **major breach** to Congress is distinct and separate from the assessment of the potential risk of harm to individuals resulting from a suspected or confirmed breach.⁴⁶

16-6. Federal Sub-agencies and Components. The FCC's sub-agencies and components may develop and implement their own BRP, but with certain caveats:⁴⁷

- (A) The FCC's SAOP must approve the Breach Response Plan (BRP) of a FCC sub-agency or component, which must also be consistent with the requirements of the FCC's BRP, OMB guidance, and applicable law.⁴⁸
- (B) The SAOP shall ensure that this BRP is reviewed no less than annually, updated if necessary, and that the date of the review is properly documented in the plan.⁴⁹
- (C) Each such contractor BRP must clearly detail the relationship between the sub-agency or contractor and the FCC's BRP.⁵⁰

16-7. Data Breach Team. The FCC is required to develop an organizational response to address any suspected or real data breach:

- (A) The FCC's **Breach Response Team (BRT or "Team")** is the group of Commission officials designated by the FCC Chairman, who are convened to evaluate and respond to a breach situation.⁵¹
- (B) The BRT members are chosen because their skills and expertise to ensure that the team can develop an effective and efficient response, including providing advice to the SAOP, in responding to a breach.⁵²
- (C) In addition to the Senior Agency Official for Privacy (SAOP) as Team Leader, the BRT includes:
 - Program Manager of the program experiencing the breach

⁴⁴ OMB Memorandum M-17-12, at 16.

⁴⁵ OMB Memorandum M-17-12, at 16.

⁴⁶ OMB Memorandum M-17-05, at 8.

⁴⁷ OMB Memorandum M-17-12, at 16.

⁴⁸ OMB Memorandum M-17-12, at 16.

⁴⁹ OMB Memorandum M-17-12, at 16.

⁵⁰ OMB Memorandum M-17-12, at 16.

⁵¹ OMB Memorandum M-17-12, at 17.

⁵² OMB Memorandum M-17-12, at 17.

- Privacy Manager (IT), BRT secretary
 - Chief Information Officer (CIO)
 - Deputy CIO for Resiliency (DCIOR)
 - Chief Information Security Officer (CISO)
 - Chief Security Officer (CSO)
 - Privacy Legal Counsel (OGC)
 - Office of Media Relations (OMR)
- (D) The SAOP, as head of the BRT, convenes the BRT and is responsible for leading the Team's response to all suspected or real the breach situations and advising the Chairman on the BRT's actions.⁵³
- (E) The criteria for convening the BRT is to be documented in the FCC Breach Response Plan.⁵⁴
- (F) The FCC's CIO, CISO, system owners, and SAOP (when a breach occurs) should determine the incident's impact level.⁵⁵
- (G) NIST has established an "incident management process" for Federal agencies to use to determine the level of impact of an incident.⁵⁶
- (H) The US-CERT National Cybersecurity Incident Scoring System (NCISS) uses these factors to assess the impact level of an incident:⁵⁷
- Functional Impact;
 - Observed Activity;
 - Location of Observed Activity;
 - Actor Characterization;
 - Information Impact;
 - Recoverability;
 - Cross-Section Dependency; and

⁵³ OMB Memorandum M-17-12, at 16.

⁵⁴ OMB Memorandum M-17-12, at 16.

⁵⁵ OMB Memorandum M-17-05, at 7.

⁵⁶ OMB Memorandum M-17-05, at 7.

⁵⁷ OMB Memorandum M-17-05, at 7.

- Potential Impact.

Note: The criteria for whether a breach constitutes a **major incident** is found in 16-2(D)

- (I) OMB guidelines recognize that the criteria for when to convene the BRT may be different for each agency according to its individual mission's specific authorities, circumstances, and risks.⁵⁸
 - (J) The SAOP may also appoint other FCC employees to the Team will possess the skills and expertise to effectively and efficiently respond to the PII Breach. For example and depending upon the specific circumstances of the breach, the SAOP may consult with:
 - Budget Center (BC), Financial Operations (FO),
 - OMD and Enterprise Acquisitions Center (EAC), and/or
 - OMD personnel to help procure services such as computer forensics, cybersecurity experts, services or call center support.
 - (H) When made aware of a report of a suspected or confirmed breach, the SAOP must first determine whether the Commission's response can be conducted at the staff level or whether the BRT should be convened.⁵⁹
 - (1) The criteria for when to convene the BRT will be based on the nature, circumstances and risks of the Breach.⁶⁰
 - (2) If the response can be conducted at the staff level, the SAOP may choose not to convene the BRT.⁶¹
- Note:** Situations that do not trigger a notification respond are found in Section 16-21.
- (3) At a minimum, the SAOP must always convene the BRT when a real or suspected breach constitutes a **major incident** and/or when it meets the criteria for reporting a "Breach to Congress."⁶²

Note: The requirements to report to Congress is found in Section 16-14.

16-8. Privacy Compliance Documentation. The SAOP should identify all the applicable privacy compliance documentation that will help the BRT to evaluate a suspected or actual breach situation.⁶³

- (A) These documents should identify:

⁵⁸ OMB Memorandum M-17-12, at 16.

⁵⁹ OMB Memorandum M-17-12, at 17.

⁶⁰ OMB Memorandum M-17-12, at 17.

⁶¹ OMB Memorandum M-17-12, at 17.

⁶² OMB Memorandum M-17-12, at 17.

⁶³ OMB Memorandum M-17-12, at 18.

- (1) What PII was potentially compromised,⁶⁴
 - (2) The population of individuals potentially affected,⁶⁵
 - (3) The purposes for which the PII was originally collected,⁶⁶
 - (4) The permitted uses and disclosures for the PII,⁶⁷ and
 - (5) Related information that is useful for developing the FCC's response.⁶⁸
- (B) The SAOP and the BRT must also consider the following:
- (1) Which systems of records notices (SORNs), privacy impact assessments (PIAs), and privacy notices/statements apply to the potentially compromised information?⁶⁹
 - (2) If the PII covered by a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act, and how will the FCC account for the disclosure, *e.g.*, is there a routine use permitting the disclosure and to whom?⁷⁰
 - (3) If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, does that information require new or revised SORNs or PIAs?⁷¹
 - (4) Are the relevant SORNs, PIAs, and privacy notices/statements accurate and up-to-date?⁷²

16-9. Technical Support for a Breach Response. Logistical and technical support are essential and necessary requirements for the BRT to respond effectively and efficiently to a breach so as to minimize the amount of staff and resources that must be committed.⁷³

- (A) The SAOP and the BRT should identify the logistical capabilities that exist at the FCC and which offices are responsible for maintaining those capabilities.
- (B) The SAOP and BRT should understand the ability of the Commission to support any resource-intensive activities necessary to provide notification requirements, guidance,

⁶⁴ OMB Memorandum M-17-12, at 18.

⁶⁵ OMB Memorandum M-17-12, at 18.

⁶⁶ OMB Memorandum M-17-12, at 18.

⁶⁷ OMB Memorandum M-17-12, at 18.

⁶⁸ OMB Memorandum M-17-12, at 18.

⁶⁹ OMB Memorandum M-17-12, at 18.

⁷⁰ OMB Memorandum M-17-12, at 18.

⁷¹ OMB Memorandum M-17-12, at 18.

⁷² OMB Memorandum M-17-12, at 18.

⁷³ OMB Memorandum M-17-12, at 13-14.

and services to individuals potentially impacted by the breach using the FCC's call centers, websites, and translation service.⁷⁴

- (C) The SAOP and BRT should work with the CIO to identify the FCC's technical remediation and forensic analysis capabilities and the B/Os that are responsible for maintaining these capabilities.⁷⁵
- (D) The SAOP, Chief Acquisition Officer (CAO), and the BRT are encouraged to consider contractors and/or other options to ensure that certain functions are immediately available during the initial, time-sensitive breach response period.⁷⁶
- (E) The SAOP and BRT should monitor the FCC's ability to gather, analyze, and preserve the evidence necessary to support an investigation and to identify and assess the risk of harm to potentially affected individuals.⁷⁷
- (F) The SAOP, BRT, CIO, and other senior FCC officials should consider asking for technical assistance from US-CERT and other Federal agencies (as appropriate) in the event of a breach.⁷⁸
- (G) The General Services Administration's (GSA) has government-wide Federal Supply Schedule "blanket protection agreements" (BPAs) for agencies to use contractors that provide comprehensive services needed to mitigate harm to those potentially impacted by a breach,⁷⁹ such as identity monitoring, credit monitoring, and other related, technical services as part of the efforts to respond to a breach.⁸⁰

16-10. Information Sharing. The SAOP and BRT also may need to examine information from various other sources to assess the full scope and ramifications of the breach situation.⁸¹

- (A) The SAOP and BRT may require access to additional information to reconcile or eliminate duplicate records, identify potentially affected individuals, and/or obtain contact information to provide notification to the affected individuals in responding to a breach.⁸²
- (B) The appropriate response may also require the Commission to combine information maintained in different information systems at the FCC, share information between agencies, and/or share information with non-Federal entities in responding to a Breach.⁸³
- (C) At a minimum the BRP requires the SAOP and the BRT to consider the following:⁸⁴

⁷⁴ OMB Memorandum M-17-12, at 14.

⁷⁵ OMB Memorandum M-17-12, at 14.

⁷⁶ OMB Memorandum M-17-12, at 14.

⁷⁷ OMB Memorandum M-17-12, at 14.

⁷⁸ OMB Memorandum M-17-12, at 14.

⁷⁹ OMB Memorandum M-17-12, at 13.

⁸⁰ OMB Memorandum M-17-12, at 13.

⁸¹ OMB Memorandum M-17-12, at 18.

⁸² OMB Memorandum M-17-12, at 18.

⁸³ OMB Memorandum M-17-12, at 18.

⁸⁴ OMB Memorandum M-17-12, at 18.

- (1) Would the information sharing be consistent with existing or require new data use agreements, information exchange agreements, or memoranda of understanding?⁸⁵
 - (2) How will PII be transmitted and protected when in transmission, for how long will it be retained, and will it be shared within the FCC and/or with outside third parties?⁸⁶
- (D) The SAOP and the BRT may also need to consult personnel at the FCC, as appropriate:
- (1) Budget and procurement personnel can provide expertise when a breach involves contractors or an acquisition, or who may help to procure services such as computer forensics, cybersecurity experts, services, or call center support;⁸⁷
 - (2) Human resources personnel can assist when employee misconduct results in a breach or when an employee is suspected of intentionally causing a breach or violating FCC policy;⁸⁸
 - (3) Law enforcement personnel can assist when a breach involves the violation or suspected violation of law or when a breach is the subject of a law enforcement investigation;⁸⁹
 - (4) Physical security personnel can investigate a breach involving unauthorized physical access to a facility or when additional information regarding physical access to a facility is required;⁹⁰ and
 - (5) Other FCC personnel who may be necessary according to specific agency missions, authorities, circumstances, and identified risks.⁹¹
- 16-11. Reporting a Suspected or Confirmed Breach. The FCC's BRP designates the Security Operation Center (SOC) as the contact point for all suspected or confirmed breaches at the Commission.⁹²
- (A) All suspected and/or real breach situations must also be reported to the **SAOP**, as the FCC's official responsible for addressing breach situations and as leader of the BRT.
 - (B) The **Chief Security Office (CSO)** handles paper-based breach incidents, and the **Chief Information Security Officer (CISO)** handles electronic/data-based breach incidents.

⁸⁵ OMB Memorandum M-17-12, at 18.

⁸⁶ OMB Memorandum M-17-12, at 18.

⁸⁷ OMB Memorandum M-17-12, at 17.

⁸⁸ OMB Memorandum M-17-12, at 17.

⁸⁹ OMB Memorandum M-17-12, at 17.

⁹⁰ OMB Memorandum M-17-12, at 17.

⁹¹ OMB Memorandum M-17-12, at 18.

⁹² OMB Memorandum M-17-12, at 19.

- (C) Employees and contractors with access to Federal information, including PII, and to the Federal information systems that handle it must report any data breach to the SOC as soon as possible and without unreasonable delay:
- (1) This requirement is consistent with the FCC's incident management policy and procedures, NIST standards and guidelines, and US-CERT notification guidelines.⁹³
 - (2) The individual(s) reporting the real or suspected breach should not wait should not wait for confirmation that a breach has occurred to report the situation to their agency:
 - (a) A delay may undermine the FCC's ability to apply preventative and remedial measures to protect the PII or reduce the risk of harm to potentially affected individuals;⁹⁴ and
 - (b) A delay may reduce the likelihood that the FCC can recover a lost or stolen device or physical document.⁹⁵
 - (3) The real or suspected breach requirement includes information contained in any medium or form, including but not limited to paper documents, oral messages, and electronic data.⁹⁶
 - (4) Prompt reporting provides the Commission with time to take steps to ameliorate the situation, such as removing information remotely from a device or enabling law enforcement to retrieve the lost or stolen equipment and PII.⁹⁷

Note: OMB recommends that Federal agencies should consider establishing a memorable e-mail address and/or toll free telephone number dedicated to incident response, such as breach@FCC.gov to enable employees and contractors to report any suspected or confirmed breach situation while in the office, teleworking, or from a remote location such as while traveling on FCC business.⁹⁸

16-12. **Reporting to US-CERT.** US-CERT must be notified of any real or suspected breach consistent with US-CERT notification guidelines and the FCC's incident management policy.⁹⁹

- (A) The SAOP should ensure that employees and contractors staffing the FCC's SOC are properly trained to identify a breach.¹⁰⁰
- (B) The SAOP and BRT will assess whether a breach constitutes a major incident based on OMB guidelines, and report the situation to US-CERT as soon as the FCC has a reasonable basis to conclude that such a breach has occurred.¹⁰¹

⁹³ OMB Memorandum M-17-12, at 14.

⁹⁴ OMB Memorandum M-17-12, at 14.

⁹⁵ OMB Memorandum M-17-12, at 14.

⁹⁶ OMB Memorandum M-17-12, at 14.

⁹⁷ OMB Memorandum M-17-12, at 14.

⁹⁸ OMB Memorandum M-17-12, at 15.

⁹⁹ OMB Memorandum M-17-12, at 19.

¹⁰⁰ OMB Memorandum M-17-12, at 19.

¹⁰¹ OMB Memorandum M-17-12, at 19.

- (C) US-CERT may help the FCC assess the circumstances that contributed to the breach and take corrective actions on technical remediation within its scope.¹⁰²
- (D) However, the FCC is ultimately responsible for responding to a breach, including full logistical and technical remediation and forensic analysis.¹⁰³

16-13. Notifying Law Enforcement, Office of Inspector General, and Office of General Counsel. An FCC's **Breach Response Plan (BNP)** should include the following:

- (A) The **BRP** will identify the FCC officials responsible for notifying and consulting with law enforcement and the Office of Inspectors General (OIG) and the Office of General Counsel (OGC) on behalf of the Commission.¹⁰⁴
- (B) The SAOP should coordinate with the SOC staff to ensure that law enforcement and OIG and OGC receive timely notification when notification is appropriate.¹⁰⁵
- (C) The SAOP should also consider and advise the appropriate officials on whether the specific circumstances and type of PII potentially compromised by a breach require the involvement of other oversight entities.¹⁰⁶
- (D) When the breach warrants a report to law enforcement, the agency should ensure that the report occurs promptly, even if the breach is unconfirmed or circumstances are unclear – prompt reporting to law enforcement can prevent PII from being further compromised and in some cases reduce the risk of harm to potentially affected individuals.¹⁰⁷
- (E) When an agency has notified law enforcement of a breach, the SAOP should consider any relevant information provided to the agency by the law enforcement that may help inform whether the breach was **intentional** or **unintentional**.¹⁰⁸

Note: Section 16-16(C) discusses intentional vs. unintentional “risk factors” in the SAOP assessment a breach.

16-14. Notifying Congress. The FCC should designate officials in the BRP who are to notify Congress.¹⁰⁹

- (A) The officials should notify the appropriate **Congressional Committees** pursuant to FISMA requirements no later than **seven days** after the date on which there is a reasonable basis to conclude that a breach constituting a “major incident” has occurred.

¹⁰² OMB Memorandum M-17-12, at 19.

¹⁰³ OMB Memorandum M-17-12, at 19.

¹⁰⁴ OMB Memorandum M-17-12, at 19.

¹⁰⁵ OMB Memorandum M-17-12, at 19.

¹⁰⁶ OMB Memorandum M-17-12, at 19.

¹⁰⁷ OMB Memorandum M-17-12, at 19.

¹⁰⁸ OMB Memorandum M-17-12, at 26.

¹⁰⁹ OMB Memorandum M-17-12, at 19.

- (B) The officials must also supplement their initial seven day Congressional notification with a report no later than **30 days** after the agency discovers the breach, consistent with FISMA requirements and OMB guidelines.¹¹⁰

16-15. Assessing the Risk to Individuals. The SAOP and the BRT will conduct an assessment of the risk of harm to individuals potentially affected as part the FCC's response to any suspected or real breach.¹¹¹

- (A) The FCC's BRP should include a list of factors to consider when assessing the potential harm to individuals resulting from the loss or compromise of their PII – these may include:¹¹²
- Breach of confidentiality or fiduciary responsibility
 - Potential for blackmail
 - Disclosure of privacy facts, mental pain, and emotional distress
 - Financial harm
 - Disclosure of contact information for victims of abuse
 - Potential for secondary uses of the information that could result in fear or uncertainty
 - Unwarranted exposure to leading to humiliation or loss of self-esteem
- (B) The SAOP and BRT must also consider any and all risks relevant to the breach, including potential risks to the FCC, its information systems, its programs and operations, the Federal Government, or national security. These additional risks can influence the FCC's overall breach response actions, including notification to individuals.¹¹³

16-16. Risk Factors. The SAOP should consider these factors when assessing the risk of harm to individuals potentially affected by a breach:

- (A) **Nature and sensitivity of the PII potentially compromised by a Breach** should be assessed for the potential harms that an individual could experience from the compromise of that type of PII:
- (1) **Data Elements** would include an analysis of the sensitivity of each individual data element as well as the sensitivity of all data elements together.¹¹⁴
- (a) **Certain data elements** are particularly sensitive and may alone present an increased risk of harm to the individual: SSNs, passport numbers, driver's license numbers, state identification numbers, bank account numbers, passwords, and biometric identification.¹¹⁵
- (b) **Multiple pieces of information**, none of which are particularly sensitive in isolation and would not pose a risk, may present an increased risk to an individual when combined: birth dates, places of birth, addresses, and

¹¹⁰ OMB Memorandum M-17-12, at 19.

¹¹¹ OMB Memorandum M-17-12, at 20.

¹¹² OMB Memorandum M-17-12, at 20.

¹¹³ OMB Memorandum M-17-12, at 21.

¹¹⁴ OMB Memorandum M-17-12, at 21.

¹¹⁵ OMB Memorandum M-17-12, at 22.

gender.¹¹⁶ In addition, information that may have been potentially compromised in a previous data breach, as well as other available information, when combined with this information may result in an increased risk of harm to the individual.¹¹⁷

- (c) **Context**, including the purpose for which the PII was collected, maintained, and used, since the same information in different contexts can reveal additional information about impacted individuals.¹¹⁸
- (2) **Private Information** should be assessed to determine the extent to which the PII, in a given context, may reveal particularly private information about an individual:¹¹⁹
 - (a) The extent to which PII constitutes information that an individual would generally keep private – harm of exposure would pose a risk of embarrassment, blackmail, or emotional distress, such as criminal information, personal debt and finances, medical conditions, sexual orientation, adoption, and/or immigration status.¹²⁰
- (3) **Vulnerable Populations** should be evaluated to determine the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population:¹²¹
 - (a) Are the potentially affected individuals from a particularly vulnerable population that may be at greater risk of harm than the general population, such as children, active duty military, government officials in sensitive positions, senior citizens, individuals with disabilities, confidential informants, witnesses, certain populations of immigrants, non-English speakers, and some crime victims.¹²²
- (4) **Permanence** of the threat should be evaluated in terms of the continued relevance and utility of the PII over time and whether it is easily replaced or substituted.¹²³
 - (a) Assessing the relevancy and utility of the information over time and whether the information will permanently identify an individual – would the risk to the information lose its relevancy or utility over time or whether it would apply to an individual throughout his/her life, such as an insurance ID that can be replaced versus an individual’s medical history.¹²⁴

¹¹⁶ OMB Memorandum M-17-12, at 22.

¹¹⁷ OMB Memorandum M-17-12, at 22.

¹¹⁸ OMB Memorandum M-17-12, at 22.

¹¹⁹ OMB Memorandum M-17-12, at 21.

¹²⁰ OMB Memorandum M-17-12, at 22.

¹²¹ OMB Memorandum M-17-12, at 21.

¹²² OMB Memorandum M-17-12, at 23.

¹²³ OMB Memorandum M-17-12, at 21.

¹²⁴ OMB Memorandum M-17-12, at 23.

- (b) Special consideration is warranted when a breach involves biometric information, including fingerprints, hand geometry, retina/iris scans, and DNA/genetic information. Consideration should also be given to current uses of the information and consider future potential uses.¹²⁵

(B) **Likelihood of Access and Use of PII** includes an assessment of how likely the breached information will be accessed and used.¹²⁶

- (1) **Security Safeguards** should be evaluated to determine whether the PII was properly encrypted or rendered partially or completely inaccessible by other means:¹²⁷

- (c) Security safeguards may significantly reduce the risk of harm to potentially affected individuals.¹²⁸
- (d) The CIO should evaluate the implementation and effectiveness of security safeguards protecting the information.¹²⁹
- (e) The CIO shall consider each of security safeguards on a case-by-case basis and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming these safeguards.¹³⁰
- (f) PII potentially compromised by a breach may also be rendered partially or completely inaccessible by security safeguards by data encryption, redaction, data masking, and remote wiping of a connected device.¹³¹
- (g) Physical security safeguards may include locked rooms with key-coded access, locked file cabinets for security documents or devices may also reduce the likelihood of access and use of PII.¹³²

- (2) **Format and Media** should be evaluated to determine whether the format of the PII may make it difficult and resource-intensive to use,¹³³

- (a) The SAOP, in coordination with the CIO, shall evaluate whether the format or media of the PII may make its use difficult and resource-intensive.¹³⁴
- (b) The format of the PII or the media on which the PII is maintained may make the PII more susceptible to a “crime of opportunity,” *e.g.*, a

¹²⁵ OMB Memorandum M-17-12, at 23.

¹²⁶ OMB Memorandum M-17-12, at 23.

¹²⁷ OMB Memorandum M-17-12, at 23.

¹²⁸ OMB Memorandum M-17-12, at 23.

¹²⁹ OMB Memorandum M-17-12, at 23.

¹³⁰ OMB Memorandum M-17-12, at 23.

¹³¹ OMB Memorandum M-17-12, at 23.

¹³² OMB Memorandum M-17-12, at 23.

¹³³ OMB Memorandum M-17-12, at 25.

¹³⁴ OMB Memorandum M-17-12, at 25.

spreadsheet on a portable USB flash drive does not require any special skill or knowledge to access that an unauthorized user could quickly search for specific data fields like SSNs.¹³⁵

- (c) The SAOP should also consider the type, value, or sensitivity of the PII: the PII's value may outweigh the difficulty and resources needed to access it and increase the likelihood of access and use regardless of its format or media.¹³⁶
- (3) **Duration of Exposure** would be a factor to consider in assessing on how long the PII was exposed.¹³⁷
 - (a) The SAOP should consider the amount of time that the PII is exposed when assessing the likelihood of access to and use of PII in evaluating a potential breach situation: the longer that PII has been exposed the more likely to have been accessed or used by unauthorized individuals.¹³⁸
- (4) **Evidence of Misuse** would help the SAOP and BRT to determine if there is any evidence confirming that the PII is being misused or that it was never accessed.¹³⁹
 - (a) The SAOP should determine whether there is evidence of misuse when assessing the likelihood of access and use of PII potentially compromised by a breach: evidence may indicate that identity theft has already occurred as a result of a specific breach or that the PII is appearing in unauthorized external contexts.¹⁴⁰
 - (b) The SAOP and the BRT should determine with reasonable certainty that PII was not misused using forensic analysis of a recovered device may reveal that PII was not accessed.¹⁴¹
- (C) The SAOP should consider the following when determining the type of breach:¹⁴²
 - (1) **Intent**, including whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown.¹⁴³
 - (a) If the breach was **intentional**, the SAOP should consider the information was the target, or whether the target was the device itself, *e.g.*, a mobile phone or laptop, and whether the compromise of the information was incidental.¹⁴⁴

¹³⁵ OMB Memorandum M-17-12, at 25.

¹³⁶ OMB Memorandum M-17-12, at 25.

¹³⁷ OMB Memorandum M-17-12, at 25.

¹³⁸ OMB Memorandum M-17-12, at 25.

¹³⁹ OMB Memorandum M-17-12, at 23.

¹⁴⁰ OMB Memorandum M-17-12, at 25 - 26.

¹⁴¹ OMB Memorandum M-17-12, at 26.

¹⁴² OMB Memorandum M-17-12, at 26.

¹⁴³ OMB Memorandum M-17-12, at 26.

¹⁴⁴ OMB Memorandum M-17-12, at 26.

- (b) While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.¹⁴⁵
 - (c) While the risk of harm to individuals may be lower when a breach is **unintentional**, either by user error or sometimes by failure to comply with the FCC's policies, the SAOP, BRT, and other Commission officials must conduct a case-by-case assessment to determine the risk of harm.¹⁴⁶
 - (d) When unable to determine if a breach was intentional or unintentional, the SAOP should give more credence to the possibility that the breach was intentional.¹⁴⁷
- (2) **Recipient**, including whether the PII is disclosed to a known or unknown recipient, and the trustworthiness of a known recipient.¹⁴⁸
- (a) Knowing who received the compromised PII helps the SAOP and the BRT to assess the likely risk of harm to individuals, such as when someone reports a breach after receiving information that he/she should not have received.¹⁴⁹
 - (b) When PII is inadvertently sent to an individual outside an agency, the risk of harm may be minimal if it is confirmed that, for example: if the individual is known to the agency, acknowledged receipt of the PII, did not forward or otherwise use the PII, and the PII was properly, completely, and permanently deleted by the recipient.¹⁵⁰
- Note:** This is a breach that must be reported within the agency and appropriately responded to, but the risk is low enough that the response often does not necessitate that the agency notify or provide services to the individual whose PII was compromised,¹⁵¹ which is found in Section 16-21.
- (c) The risk of harm to an individual is much higher if analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information.¹⁵²
 - (d) The SAOP should rely on the various factors and circumstances enumerated above to assess the harm and to determine the appropriate action to take when an agency does not have any information indicating that compromised or lost PII was ever received or acquired by anyone.¹⁵³

¹⁴⁵ OMB Memorandum M-17-12, at 26.

¹⁴⁶ OMB Memorandum M-17-12, at 26.

¹⁴⁷ OMB Memorandum M-17-12, at 26.

¹⁴⁸ OMB Memorandum M-17-12, at 26.

¹⁴⁹ OMB Memorandum M-17-12, at 27.

¹⁵⁰ OMB Memorandum M-17-12, at 27.

¹⁵¹ OMB Memorandum M-17-12, at 27.

¹⁵² OMB Memorandum M-17-12, at 27.

¹⁵³ OMB Memorandum M-17-12, at 27.

16-17. Mitigating the Risk to Individuals. The SAOP and the BRT should consider how to mitigate the impacts on individuals based on their risk assessment.¹⁵⁴

- (A) The SAOP and the BRT should advise the FCC Chairman on whether to take counter measures, offer guidance, or provide services to individuals affected by the breach.¹⁵⁵
- (B) Since each breach is “fact-specific,” the decision about offering guidance or providing services depends upon the breach’s circumstances.¹⁵⁶
- (C) The FCC should consider the assessed risk of harm based on:
 - Nature and sensitivity of the PII,
 - Likelihood of access and use of the PII, and/or
 - Type of breach.¹⁵⁷
- (D) Assessed risk of harm to individuals should inform the FCC’s decision on whether or not to offer guidance or to provide services.¹⁵⁸
- (E) The FCC Chairman (or his/her designee, *i.e.*, SAOP) is ultimately responsible for making the final decision on providing guidance and/or services to these individuals impacted by the breach.¹⁵⁹
- (F) The SAOP should determine and document the FCC’s actions that are taken to mitigate the risk of harm, which can include.¹⁶⁰
 - (1) **Countermeasures**, such as expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII,¹⁶¹
 - (a) Countermeasures may not always prevent harm to potentially affected individuals, but they may limit or reduce the risk of harm.¹⁶²
 - (b) If the information is only useful in a specific context, there may be context-specific countermeasures that can be taken to limit risk of harm, such as changing passwords, closing and re-issuing accounts, and/or identity and/or credit monitoring are countermeasures that may be needed.¹⁶³
 - (2) **Guidance**, such as how individuals may obtain a free credit report and whether they should consider closing certain accounts;¹⁶⁴

¹⁵⁴ OMB Memorandum M-17-12, at 27.

¹⁵⁵ OMB Memorandum M-17-12, at 27.

¹⁵⁶ OMB Memorandum M-17-12, at 27.

¹⁵⁷ OMB Memorandum M-17-12, at 27.

¹⁵⁸ OMB Memorandum M-17-12, at 27.

¹⁵⁹ OMB Memorandum M-17-12, at 27.

¹⁶⁰ OMB Memorandum M-17-12, at 27.

¹⁶¹ OMB Memorandum M-17-12, at 27.

¹⁶² OMB Memorandum M-17-12, at 27.

¹⁶³ OMB Memorandum M-17-12, at 28.

¹⁶⁴ OMB Memorandum M-17-12, at 28.

- (a) The SAOP should consider what guidance to provide to both FCC employees and contractors and other individuals about how they may mitigate their own risk of harm, including:¹⁶⁵

- Adding multi-factor identification for FCC account access;
- Changing passwords frequently;
- Setting up fraud alerts or credit freezes;
- Changing or closing accounts that may have been affected; and/or
- Using Federal Trade Commission (FTC) services.¹⁶⁶

Note: The FTC provides specific guidance when a breach involves SSNs, payment card information, bank accounts, driver's licenses, children's information, and account credentials.¹⁶⁷

- (b) The guidance will necessarily depend upon the potentially compromised information.¹⁶⁸

- (c) Agencies should use the information available at www.IdentityTheft.gov/databreach as the baseline for drafting guidance.¹⁶⁹

(3) **Services**, such as identity and/or credit monitoring.¹⁷⁰

- (a) The SAOP should determine if there are services the agency can provide.¹⁷¹
- (b) The SAOP should identify those services that best mitigate the specific risk of harm resulting from the circumstances surrounding the particular breach and make recommendations accordingly.¹⁷²
- (c) If it is determined that no services should be provided, notification to affected individuals is still required.¹⁷³

16-18. Notification to Affected Individuals. The SAOP and the BRT are responsible for advising the FCC Chairman on whether and when to notify the affected individuals.¹⁷⁴

¹⁶⁵ OMB Memorandum M-17-12, at 28.

¹⁶⁶ OMB Memorandum M-17-12, at 28.

¹⁶⁷ OMB Memorandum M-17-12, at 28.

¹⁶⁸ OMB Memorandum M-17-12, at 28.

¹⁶⁹ OMB Memorandum M-17-12, at 28.

¹⁷⁰ OMB Memorandum M-17-12, at 28.

¹⁷¹ OMB Memorandum M-17-12, at 28.

¹⁷² OMB Memorandum M-17-12, at 28.

¹⁷³ OMB Memorandum M-17-12, at 28.

¹⁷⁴ OMB Memorandum M-17-12, at 29.

- (A) When notification is necessary, helpful, or otherwise required, the **FCC Chairman** or another senior-level FCC official (designated in writing, *e.g.*, SAOP or the Managing Director) should notify the potentially affected individuals.¹⁷⁵
- (B) Notification should be based on an assessment of the breach situation and done in a way appropriate to the circumstances of the potential breach. Individuals should be advised of the FCC's mitigation plan and the assessed risk of harm to them.¹⁷⁶
- (C) OMB advises agencies to balance the need for transparency with concerns about over-notifying individuals.¹⁷⁷
- (D) Notification may not always be helpful to the potentially affected individuals, and the SAOP and BRT should exercise care to evaluate the benefit of providing notice to individuals or notifying the public.¹⁷⁸
- (E) Since certain Federal information systems may be subject to other breach notification requirements, the SAOP should ensure that appropriate subject matter experts can identify those requirements are part of the BRT.¹⁷⁹
- (F) When multiple notification requirements may apply to a breach, the Commission should provide a single notice to potentially affected individuals that complies with the guidance in OMB Memorandum M-17-12 and all other applicable notification requirements.¹⁸⁰

16-19. Notification Procedures. When it is necessary to notify individuals potentially affected by a breach, the SAOP and the BRT should coordinate the FCC's notification procedure(s), including:¹⁸¹

- (A) **Source of the Notification** to the potentially affected individuals should be determined by the FCC Chairman or his/her designee (senior-level FCC official such as the SAOP):¹⁸²
 - (1) Notification from this level demonstrates that the breach is a Commission priority.¹⁸³
 - (2) The SAOP may issue the notification when a small number of individuals are potentially affected by a breach, and the SAOP determines that there is only a low risk of harm to them.¹⁸⁴

Note: Information concerning situations that do not trigger a notification are in Section 16-21.

¹⁷⁵ OMB Memorandum M-17-12, at 30.

¹⁷⁶ OMB Memorandum M-17-12, at 29.

¹⁷⁷ OMB Memorandum M-17-12, at 29.

¹⁷⁸ OMB Memorandum M-17-12, at 29.

¹⁷⁹ OMB Memorandum M-17-12, at 29.

¹⁸⁰ OMB Memorandum M-17-12, at 29 -30.

¹⁸¹ OMB Memorandum M-17-12, at 29 -30.

¹⁸² OMB Memorandum M-17-12, at 29 -30.

¹⁸³ OMB Memorandum M-17-12, at 29 -30.

¹⁸⁴ OMB Memorandum M-17-12, at 29 -30.

- (3) The SAOP and the BRT will oversee the notification process for potentially affected individuals for any breach that involves a contractor working on behalf of the.¹⁸⁵
- (B) **Timeliness of the Notification** should be done as expeditiously as practicable, without unreasonable delay;¹⁸⁶
- (1) OMB advises agencies to avoid providing multiple notifications for a single breach and to balance the timeliness of the notification with the need to gather and confirm information about a breach and to assess the risk of harm to potentially affected individuals.¹⁸⁷
 - (2) The FCC Chairman may consider whether the issue has been corrected or resolved prior to providing notification when a technical issue contributed to the breach.¹⁸⁸
- Note:** The U.S. Attorney General, head of an element of the Intelligence Community, or the Secretary of DHS may delay notifying individuals potentially affected by a breach if the notification would disrupt law enforcement investigation, endanger national security, or hamper security remediation actions.¹⁸⁹
- (3) The SAOP should notify the FCC Chairman when it is decided to delay notification to the affected individuals.¹⁹⁰
- (C) **Contents of the Notification** should consider these factors:¹⁹¹
- (1) The FCC's notification to individuals potentially affected by a breach with notification should be concise and use plain language that avoids jargon.¹⁹²
 - (2) The notification should avoid generic or repetitive language and should be tailored to the notification to the specific breach.¹⁹³
 - (3) It may be necessary for to draft different notifications for different populations affected by the same breach.¹⁹⁴
 - (4) At a minimum the notification should include the following:¹⁹⁵
 - A brief description of what happened, including the date(s) of the breach and its discovery;¹⁹⁶

¹⁸⁵ OMB Memorandum M-17-12, at 29 -30.

¹⁸⁶ OMB Memorandum M-17-12, at 31.

¹⁸⁷ OMB Memorandum M-17-12, at 31.

¹⁸⁸ OMB Memorandum M-17-12, at 31.

¹⁸⁹ OMB Memorandum M-17-12, at 31.

¹⁹⁰ OMB Memorandum M-17-12, at 31.

¹⁹¹ OMB Memorandum M-17-12, at 31.

¹⁹² OMB Memorandum M-17-12, at 31.

¹⁹³ OMB Memorandum M-17-12, at 31.

¹⁹⁴ OMB Memorandum M-17-12, at 31.

¹⁹⁵ OMB Memorandum M-17-12, at 31.

¹⁹⁶ OMB Memorandum M-17-12, at 31.

- To the extent possible, it should include a description of the types of PII compromised by the breach (*e.g.*, full name, SSN, date of birth, home address, account number(s), and disability code);¹⁹⁷
 - A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information systems;¹⁹⁸
 - Guidance to potentially affected individuals on how they can mitigate their own risk of harm, counter measures the FCC is taking, and services the FCC is providing to potentially affected individuals, if any;¹⁹⁹
 - Steps the FCC is taking, if any, to investigate the breach, to mitigate losses, and to protect against a future breach;²⁰⁰ and
 - Whom should potentially affected individuals contact at the FCC for more information, including a telephone number (preferably toll-free), e-mail address, and postal address.²⁰¹
- (5) Agencies may want to provide additional details in a Frequently Asked Questions (FAQ) format on the agency website or via an enclosure.
- (a) The FAQs on an agency website may be more beneficial because:
- It can be easily update,²⁰²
 - It can contain links to more information,²⁰³
 - It can provide more tailored information than the formal notification,²⁰⁴ and
 - It can be easily translated into multiple languages.²⁰⁵
- (b) For wide-spread breaches affecting a large number of individuals, OMB suggest that a toll-free numbers be established that is staffed by trained personnel to handle inquiries from the affected individuals;²⁰⁶

¹⁹⁷ OMB Memorandum M-17-12, at 31.

¹⁹⁸ OMB Memorandum M-17-12, at 31.

¹⁹⁹ OMB Memorandum M-17-12, at 32.

²⁰⁰ OMB Memorandum M-17-12, at 32.

²⁰¹ OMB Memorandum M-17-12, at 32.

²⁰² OMB Memorandum M-17-12, at 32.

²⁰³ OMB Memorandum M-17-12, at 32.

²⁰⁴ OMB Memorandum M-17-12, at 32.

²⁰⁵ OMB Memorandum M-17-12, at 32.

²⁰⁶ OMB Memorandum M-17-12, at 32.

- (c) Notification, as appropriate, should also be available in the appropriate languages to the extent feasible;²⁰⁷
 - (d) The SAOP and BRT may seek additional guidance on how to draft notification from the FTC, as well as communications experts.²⁰⁸
- (D) **Method of Notification** should be determined by the SAOP and include consideration of the best method(s) for providing notification depending on the circumstances of a breach, depending upon:²⁰⁹
 - The number of individuals affected,
 - The available contact information for the potentially affected individuals, and
 - The urgency with which the individuals need to receive the notification.²¹⁰
- (E) The means to notify including:²¹¹
 - (1) **First-Class Mail:**
 - (a) First-class notification to the last known mailing address of the individual in agency records should be the primary means by which notification is provided.²¹²
 - (b) Where the agency has reason to believe the address is no longer current, reasonable steps should be taken to update the address by consulting with other agencies such as the USPS.²¹³
 - (2) **Telephone:**
 - (a) Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a small number of individuals are affected.
 - (b) Telephone notification should be contemporaneous with written notification by first-class mail.²¹⁴
 - (3) **E-mail:**

²⁰⁷ OMB Memorandum M-17-12, at 32.

²⁰⁸ OMB Memorandum M-17-12, at 32.

²⁰⁹ OMB Memorandum M-17-12, at 32.

²¹⁰ OMB Memorandum M-17-12, at 32.

²¹¹ OMB Memorandum M-17-12, at 32.

²¹² OMB Memorandum M-17-12, at 32.

²¹³ OMB Memorandum M-17-12, at 32.

²¹⁴ OMB Memorandum M-17-12, at 33.

- (a) E-mail notification, especially to or from a non-government e-mail address, is not recommended due to the high risk of malicious e-mail attacks that are often launched when attackers hear about a breach.²¹⁵
- (b) E-mails often do not reach individuals because they are automatically routed to spam or junk mail folders.²¹⁶
- (c) Individuals who receive notifications via e-mail are often uncertain of the legitimacy of the e-mail and will not open the notification.²¹⁷
- (d) While e-mail is not recommended as the primary form of notification, in limited circumstances, it may be appropriate, such as an intra-office or intra-agency notification for small groups.²¹⁸

(4) **Substitute Notification:**

- (a) The SAOP and BRT may determine that the Commissions will provide substitute notifications if there is insufficient contact information to provide notification, and also as supplemental notification for any breach to keep potentially affected individuals informed.²¹⁹
- (b) A substitute notification may also be beneficial if the agency needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly sensitive.²²⁰
- (c) A substitute notification should consist of a conspicuous posting of the notification on the home page of the agency's website and/or notification to major print and broadcast media, including major media in the areas where the potentially affected individuals reside.²²¹
- (d) Notification to media should include a toll-free number and/or an e-mail address that an individual can use to learn whether his/her personal information is affected by the breach.²²²
- (e) Agencies should consider whether it is appropriate to establish an on-going communication method for interested individuals to automatically receive updates when there is an on-going investigation and the facts and circumstance of a breach are evolving.²²³

²¹⁵ OMB Memorandum M-17-12, at 33.

²¹⁶ OMB Memorandum M-17-12, at 33.

²¹⁷ OMB Memorandum M-17-12, at 33.

²¹⁸ OMB Memorandum M-17-12, at 33.

²¹⁹ OMB Memorandum M-17-12, at 33.

²²⁰ OMB Memorandum M-17-12, at 33.

²²¹ OMB Memorandum M-17-12, at 33.

²²² OMB Memorandum M-17-12, at 33.

²²³ OMB Memorandum M-17-12, at 33.

- (f) Depending upon the circumstances of the breach and individuals affected, agencies may need to provide notification in more than one language.²²⁴
- (F) **Special Considerations** may include tailoring the notification for vulnerable populations, and determining whether to provide notification to individuals other than those whose PII was potentially compromised, and how to notify individuals who are visually or hearing impaired.²²⁵
 - (1) The SAOP and BRT may determine that the Commission needs to provide a different type of notification to individuals in vulnerable populations like children and those with special needs, or to provide notification when it would not otherwise be necessary.²²⁶
 - (2) The Commission may also need to provide notification to individuals other than or in addition to those whose PI was potentially compromised, such as children or those with special needs, and determine who the other appropriate individuals are, such as parents, guardians, and other care-givers.²²⁷
 - (3) The Commission should also determine whether to give special consideration to providing notice to individuals who are visually or hearing impaired, consistent with Section 508 of the *Rehabilitation Act of 1973*, as amended, including use of telecommunications devices for the deaf (TDD) or large-type notices on the agency website.²²⁸

16-20. Tracking and Documenting Notifications. The SAOP will direct the BRT and the Security Operations Center (SOC) in developing and maintaining a formal process to track and document each suspected or confirmed breach as provided in the BRP.²²⁹

- (A) This process is to ensure that the SAOP is made aware of each report of a suspected or confirmed breach in a timely manner.²³⁰
- (B) The SAOP is responsible for keeping the SOC informed of the status of an on-going response and for determining when the response to a breach has concluded.²³¹
- (C) The SAOP is to report to the SOC:
 - (a) The status of the FCC's response to a breach,²³² and
 - (b) The outcome of the response upon its conclusion.²³³

²²⁴ OMB Memorandum M-17-12, at 33.

²²⁵ OMB Memorandum M-17-12, at 33.

²²⁶ OMB Memorandum M-17-12, at 33.

²²⁷ OMB Memorandum M-17-12, at 33 - 34.

²²⁸ OMB Memorandum M-17-12, at 34.

²²⁹ OMB Memorandum M-17-12, at 34.

²³⁰ OMB Memorandum M-17-12, at 34.

²³¹ OMB Memorandum M-17-12, at 34.

²³² OMB Memorandum M-17-12, at 34.

²³³ OMB Memorandum M-17-12, at 34.

- (D) OMB recommends that a standard internal reporting template be used that includes a comprehensive list of data elements and information types to reflect its mission and functions as part of its responsibility for internal tracking and documenting its breach response procedures.²³⁴
- (E) The process for internally tracking each reporting breach enables the FCC to track and monitor the following:²³⁵
 - (1) The total number of suspected and real breaches reported over a given time period;²³⁶
 - (2) The status for each reported or suspected breach, including whether the FCC's response to a breach is on-going or has concluded;²³⁷
 - (3) The number of individuals potentially affected by each reported breach;²³⁸
 - (4) The types of information potentially compromised by each reported breach;²³⁹
 - (5) Whether the FCC, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach;²⁴⁰
 - (6) Whether the FCC, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach;²⁴¹ and
 - (7) Whether a breach was reported to US-CERT and/or Congress.²⁴²

16-21. Situations That Do Not Trigger Notification. The SAOP may determine that in some situations a real or confirmed breach need not be reported based on several factors:²⁴³

- (A) The SAOP will conduct an assessment of the situation, the circumstances of the suspected or confirmed breach, and evaluate the potential risks and impacts that may cause harm.²⁴⁴
- (B) Based on SAOP's assessment, guidance will be issued to employees and contractors concerning why it was not necessary to report this situation as a suspected or confirmed breach. The assessment should be based on the following:²⁴⁵
 - (1) The potential harm to individuals is negligible;²⁴⁶ and/or

²³⁴ OMB Memorandum M-17-12, at 34.

²³⁵ OMB Memorandum M-17-12, at 34.

²³⁶ OMB Memorandum M-17-12, at 34.

²³⁷ OMB Memorandum M-17-12, at 34.

²³⁸ OMB Memorandum M-17-12, at 34.

²³⁹ OMB Memorandum M-17-12, at 34.

²⁴⁰ OMB Memorandum M-17-12, at 34.

²⁴¹ OMB Memorandum M-17-12, at 35.

²⁴² OMB Memorandum M-17-12, at 35.

²⁴³ OMB Memorandum M-17-12, at 15.

²⁴⁴ OMB Memorandum M-17-12, at 15.

²⁴⁵ OMB Memorandum M-17-12, at 15.

²⁴⁶ OMB Memorandum M-17-12, at 15.

- (2) The failure to report the occurrence does not violate any laws or regulations.²⁴⁷
- (C) The FCC must document the circumstances that it has determined obviate the requirement to report a suspected or confirmed breach in the Commission's incident management policy.²⁴⁸
- 16-22. Chief Acquisition Officer's Requirements. The Chief Acquisition Officer (CAO) should coordinate with the SAOP and OGC when drafting FCC's contracts to ensure that each contract's provisions include uniform language concerning the appropriate response in case of a real or suspected breach situation.²⁴⁹
- (A) Lack of uniformity in contracts could pose serious complications in the FCC's response to any breach situation.²⁵⁰
- (B) The SAOP and CIO should ensure that the BRP and system security authorization documentation clearly define the roles and responsibilities of contractors that operate the FCC's information systems that collect, use, maintain, store, and dispose of PII on behalf of the Commission.²⁵¹
- (C) These responsibilities should also be clearly defined in the contract to ensure compliance with FCC requirements.²⁵²
- 16-23. Contractor Requirements. The contract terms for FCC contractors who handle PII should include the necessary terms for the Commission to respond appropriately to any breach situation:²⁵³
- (A) Contractors are required to cooperate with and exchange information with Commission officials, as the FCC determines are necessary, to report effectively and to manage a suspected or confirmed breach.²⁵⁴
- (B) Contractors and subcontractors must properly encrypt PII in accordance with Federal and FCC applicable policies and requirement for protecting PII.²⁵⁵
- (C) Contractors and subcontractors are required to take the FCC's privacy training courses to learn how to identify and report a breach.²⁵⁶
- Note:** The FCC's training requirements for employees and contractors are found in 16-26 and Chapter 15.
- (D) The FCC's incident management policy and US-CERT notification guidelines requires contractors and subcontractors to report all suspected or confirmed breaches in any

²⁴⁷ OMB Memorandum M-17-12, at 15.

²⁴⁸ OMB Memorandum M-17-12, at 15.

²⁴⁹ OMB Memorandum M-17-12, at 12.

²⁵⁰ OMB Memorandum M-17-12, at 12.

²⁵¹ OMB Memorandum M-17-12, at 12.

²⁵² OMB Memorandum M-17-12, at 12.

²⁵³ OMB Memorandum M-17-12, at 11.

²⁵⁴ OMB Memorandum M-17-12, at 12.

²⁵⁵ OMB Memorandum M-17-12, at 12.

²⁵⁶ OMB Memorandum M-17-12, at 12.

medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay.²⁵⁷

- (E) Contractors and subcontractors must maintain capabilities to:
- Determine what Federal information was or could have been assessed and by whom, Construct a timeline of user activity,
 - Determine methods and techniques used to access Federal information, and
 - Identify the initial attack vector.²⁵⁸

- (F) All FCC contracts for all contractors and subcontractors (at all levels) should include the appropriate language allowing the FCC to inspect, investigate, undertake forensic analysis, and any other actions necessary to ensure compliance with OMB regulations.²⁵⁹

Note: The FCC will ensure that all contracts covering contractors and subcontractors who interact with PII as part of their duties and responsibilities must include the appropriate language under the FAR clauses, 52.224-1 and 52.224-2. *See* 48 CFR §§ 52.224-1 and 52.224-2.

- (G) The FCC's BRP should identify the roles and responsibilities for contractors, in accordance with FCC policies and OMB regulations.²⁶⁰

- (H) The FCC will also remind contractors and subcontractors, as well as Commission employees, that reporting a breach is not, by itself, to be interpreted as evidence that they have failed to provide adequate safeguards for PII.²⁶¹

16-24. Grants and Grantee Requirements. Any grant recipient that uses or operates a FCC information system, or handles and/or disposes of PII within the scope of an award from the Commission must have procedures in place.²⁶²

- (B) To respond to a breach and include terms and conditions requiring the grant recipient to notify the FCC in the event of a breach; and²⁶³
- (C) To promote cooperation and the free exchange of information with Commission officials, as appropriate, to properly escalate, refer, and respond to a breach.²⁶⁴

16-25. Routine Uses. Federal agencies are required to include **two routine uses** in all system of records notices (SORNs) to address the disclosure of information from a system when necessary to respond to a breach either of the Commission's PII or, as appropriate, to assist another Federal agency in its response to a breach.²⁶⁵

²⁵⁷ OMB Memorandum M-17-12, at 12.

²⁵⁸ OMB Memorandum M-17-12, at 12.

²⁵⁹ OMB Memorandum M-17-12, at 12.

²⁶⁰ OMB Memorandum M-17-12, at 12.

²⁶¹ OMB Memorandum M-17-12, at 12.

²⁶² OMB Memorandum M-17-12, at 13.

²⁶³ OMB Memorandum M-17-12, at 13.

²⁶⁴ OMB Memorandum M-17-12, at 13.

²⁶⁵ OMB Memorandum M-17-12, at 11.

- (A) One **routine use**'s purpose is to facilitate the Commission's response to a breach of FCC records:²⁶⁶

To appropriate agencies, entities, and person when (1) the Commission suspects or has confirmed that there has been a breach of the system of records; (2) the Commission has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Commission (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with Commission efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.²⁶⁷

- (B) The other new **routine use**'s purpose is to ensure that Federal agencies are able to disclose records in their systems of records that may reasonably be needed by another agency in responding to a breach, which assists the other agency in locating or contacting individuals potentially affected by a breach or information that is related to the other agency's programs or information.²⁶⁸

To another Federal agency or Federal entity, when the Commission determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.²⁶⁹

16-26. Training. All employees, contractors, and even those with only temporary access to the information in the FCC's information systems, must receive basic information on data breaches:²⁷⁰

- (A) Information will be included in all three levels of privacy training, including initial training for new employees and contractors, annual training, and specialized training for supervisors and those whose job duties and responsibilities provide them with regular access to PII.
- (B) Instruction will give guidance on the best practices when accessing PII in the Commission's information systems that contain this sensitive information.²⁷¹
- (C) Training will inform everyone on how to identify and respond to a breach, including the basic information that must be learned as part of the Commission's internal process for reporting a data breach.²⁷²

²⁶⁶ OMB Memorandum M-17-12, at 11.

²⁶⁷ OMB Memorandum M-17-12, at 11.

²⁶⁸ OMB Memorandum M-17-12, at 11.

²⁶⁹ OMB Memorandum M-17-12, at 11.

²⁷⁰ OMB Memorandum M-17-12, at 10.

²⁷¹ OMB Memorandum M-17-12, at 10.

²⁷² OMB Memorandum M-17-12, at 10.

- (D) Training emphasizes each person's obligation to report not only a confirmed breach, but also a suspected breach involving information in any medium or form – including both electronic data, oral, visual, and paper document formats.²⁷³

Note: Each training course requires the individual to pass a test to receive course credit.

- (E) The Commission also provides on-going campaign to make everyone aware the seriousness of any real and suspected data breach situations with posters, periodic e-mails, and other methods as constant reminders.²⁷⁴

16-27. Rules of Behavior. The FCC will establish rules of behavior, including consequences for violating such rules, for employees, contractors, and all other individuals with access to Federal information and Federal information systems.²⁷⁵

- (D) The FCC requires employees and contractors to read, understand, and agreed to abide by these requirements before being given access to the Commission's information systems (including both electronic and paper-based systems and files) and the PII they contain.²⁷⁶
- (E) The FCC's rules of behavior include the consequences for those who fail to comply with these requirements.²⁷⁷

16-28. Reporting Requirements. The FCC has the following reporting and notification requirements:²⁷⁸

- (A) At the end of each quarter of the fiscal year, the FCC's SOC should report to the SAOP the status of each breach reported to the SOC during the fiscal year.²⁷⁹
- (B) The SAOP is to review and validate that the quarterly report is an accurate reflection of the status of each reported breach.²⁸⁰
- (C) The SAOP should convene the FCC's BRT to formally review the FCC's response to the breach and identify any lessons learned as part of the agency's breach report to Congress. This assessment must:²⁸¹
 - (1) Po provide an opportunity for an evaluation of the FCC's response to the breach and to implement specific, preventive actions;²⁸²
 - (2) Document any changes to its breach response plan, policies, training, or other documentation resulting from lessons learned;²⁸³ and

²⁷³ OMB Memorandum M-17-12, at 10.

²⁷⁴ OMB Memorandum M-17-12, at 10.

²⁷⁵ OMB Memorandum M-17-12, at 15.

²⁷⁶ OMB Memorandum M-17-12, at 15.

²⁷⁷ OMB Memorandum M-17-12, at 15.

²⁷⁸ OMB Memorandum M-17-12, at 35.

²⁷⁹ OMB Memorandum M-17-12, at 35.

²⁸⁰ OMB Memorandum M-17-12, at 35.

²⁸¹ OMB Memorandum M-17-12, at 35.

²⁸² OMB Memorandum M-17-12, at 35.

²⁸³ OMB Memorandum M-17-12, at 35.

- (3) Include any specific challenges that prevent the FCC from instituting remedial measures and documentation of those challenges.²⁸⁴

16-29. Tabletop Exercises. OMB requires the SAOP in each Federal agency to convene their BRT at least once annually to hold a “tabletop exercise.”²⁸⁵

- (A) The exercise will test the FCC’s breach response plan and will help to ensure that the BRT members are familiar with the plan and understand their specific roles.²⁸⁶

- (B) The exercise should be used:

- (1) To practice a coordinated response to a breach;²⁸⁷
- (2) To further refine and validate the breach response plan;²⁸⁸ and
- (3) To identify potential weaknesses in the FCC’s response capabilities.²⁸⁹

16-30. Annual BRP Reviews. OMB requires the SAOP to review the agency’s quarterly SOC breach response reports at the end of each year.²⁹⁰

- (A) The SAOP’s review should include consideration of whether the FCC should undertake any of the following actions:²⁹¹

- (1) Update the breach response plan;²⁹²
- (2) Develop and implement new policies to protect the FCC’s PII holdings;²⁹³
- (3) Reinforce existing policies to protect the FCC’s PII holdings;²⁹⁴
- (4) Modify information sharing agreements;²⁹⁵ and
- (5) Develop or revise documentation such as SORNs, PIAs, and/or privacy policies.²⁹⁶

- (B) The SAOP should also review that FCC’s BRP to confirm that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology.²⁹⁷

²⁸⁴ OMB Memorandum M-17-12, at 35.

²⁸⁵ OMB Memorandum M-17-12, at 35.

²⁸⁶ OMB Memorandum M-17-12, at 35.

²⁸⁷ OMB Memorandum M-17-12, at 35.

²⁸⁸ OMB Memorandum M-17-12, at 35.

²⁸⁹ OMB Memorandum M-17-12, at 35.

²⁹⁰ OMB Memorandum M-17-12, at 35.

²⁹¹ OMB Memorandum M-17-12, at 35.

²⁹² OMB Memorandum M-17-12, at 35.

²⁹³ OMB Memorandum M-17-12, at 35.

²⁹⁴ OMB Memorandum M-17-12, at 35.

²⁹⁵ OMB Memorandum M-17-12, at 35.

²⁹⁶ OMB Memorandum M-17-12, at 35.

²⁹⁷ OMB Memorandum M-17-12, at 36.

- (C) The SAOP is responsible for documenting the date of the most recent review and submitting the updated version of the plan to OMB when requested as part of the annual FISMA reporting.²⁹⁸

16-31. Annual FISMA Reporting. FISMA requires the FCC to submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, including a description of major information security incidents and major incidents that involved a breach.²⁹⁹

- (A) Describe the FCC's implementation of the requirements of OMB Memorandum M-17-12.
- (B) Confirm that the FCC satisfied all requirements in OMB Memorandum M-17-12 for training and awareness with respect to breach reporting, or if not, explain why it did not satisfy these requirements and what steps will be taken to satisfy the requirements in the next reporting period;³⁰⁰
- (C) Submit these statistics:
- The number of FCC breaches during the reporting period,³⁰¹
 - The number of breaches reported by the SOC to US-CERT,³⁰²
 - The number of breaches reported to Congress,³⁰³ and
 - The number of individuals potentially affected.³⁰⁴
- (D) Submit the FCC's breach response plan and certify that the plan has been reviewed and updated over the past 12 months, as appropriate.³⁰⁵
- (E) Submit the names and titles of the individuals in the FCC's BRT and identify those individuals who were removed from the team or added to the team over the past 12 months;³⁰⁶ and
- (F) Confirm that the members of the BRT participated in at least one tabletop exercise during the reporting period or, if not, explain why and what steps the FCC will take to ensure that the BRT participates in a tabletop exercise during the next reporting period.³⁰⁷

²⁹⁸ OMB Memorandum M-17-12, at 36.

²⁹⁹ OMB Memorandum M-17-12, at 36.

³⁰⁰ OMB Memorandum M-17-12, at 36.

³⁰¹ OMB Memorandum M-17-12, at 36.

³⁰² OMB Memorandum M-17-12, at 36.

³⁰³ OMB Memorandum M-17-12, at 36.

³⁰⁴ OMB Memorandum M-17-12, at 36.

³⁰⁵ OMB Memorandum M-17-12, at 36.

³⁰⁶ OMB Memorandum M-17-12, at 36.

³⁰⁷ OMB Memorandum M-17-12, at 36.

APPENDIX 1

GUIDELINES FOR PROTECTING SOCIAL SECURITY NUMBERS (SSNs) AND OTHER PERSONALLY IDENTIFIABLE INFORMATION (PII)¹

Policy. OPM has issued policy guidelines to help Federal agencies achieve a consistent and effective policy for safeguarding Social Security Numbers (SSNs) of Federal employees. The intent of this guidance is to minimize the risk of identity theft and fraud by:

- (1) Eliminating the unnecessary use of SSNs as an identifier, whenever feasible; and
- (2) Strengthening the protection of personally identifiable information (PII), including SSN data from theft or loss.
- (3) The FCC will incorporate these OPM guidelines in its privacy policies and programs.

FCC Privacy Policy Guidelines:

- (1) If Social Security Numbers (SSNs) are collected, they should be collected at the time of an employee's appointment and entered into the human resources and payroll systems.
 - (a) Paper documents with SSNs should be stored in a secure location until the documents are no longer required; and
 - (b) Disposal of paper documents with SSN data must be disposed of in accordance with the applicable General Records Schedule (GRS) issued by the National Archives and Records Administration.
- (2) Each bureau and office (B/O) should:
 - (a) Avoid unnecessary printing and displaying of SSNs on forms and reports; and
 - (b) SSN data should not be displayed on computer screens.
- (3) Access to SSN data should be restricted to only those individuals whose official duties require such access.
- (4) Each B/O should maintain a list of employees and contractors who are authorized to have access to SSN data. (This list should be updated regularly.)
- (5) Individuals who are authorized to access SSN data should understand their responsibility to protect sensitive and personal information.
- (6) Privacy training should include information on an employee's responsibility to be aware of keeping SSN data secure both in their office/workstation and when they telework.

¹ OPM Memorandum, *Guidance on Protecting Employee Social Security Numbers and Combatting Identity Theft*, June 18, 2007, at 2-3.

- (7) Privacy and confidentiality statements that describe accountability clearly and warn of possible disciplinary action for unauthorized release of SSN data and other PII should be signed by all individuals with access to this information.
- (8) The Commission's telework policies and written agreements must comply with Federal agency privacy protection policies, including policies governing the protection of SSN data when employees are teleworking from home or another approved telework location.
- (9) Each B/O should require its employees to obtain supervisory approval before they are authorized to access, transport, or transmit information or equipment containing SSN data outside agency facilities.
- (10) The Commission will ensure that electronic records containing SSN data are transported or transmitted in an encrypted or protected format as prescribed in current OMB guidance regarding the protection of sensitive agency information.
- (11) The Commission will ensure that paper-based records containing SSN data are transported in wheeled containers, portfolios, briefcases, or similar devices, which are locked when the records are not in use. These containers should be identified by tag, label, or decal with contact and mailing information.
- (12) Each B/O should ensure that required access to SSN data, including data entry, printing, and screen displays must be conducted in a secure location to protect against unauthorized exposures.
- (13) All security incidents involving PII, especially SSN data, must be reported in accordance with current OMB guidance regarding the "breach notification" protocols. In addition, all individuals authorized to access SSN data must be familiar with these incident reporting requirements.
- (14) All disclosures of information containing SSN data and other PII must be made in accordance with established regulations and procedures.
- (15) Each B/O should work with the SAOP and privacy officials to draft written procedures describing the proper labeling, storage, and disposal of printed materials containing SSN and other PII data. In particular, B/O employees with access to the SSN and other PII data should be reminded frequently of the serious potential consequences resulting from the unintended disclosure of such data.
- (16) When SSN data are required as data entry parameters, they should not be displayed on the input screen except when establishing the initial human resource or payroll records. In all record retrieval and access authorizations processes, SSN data should be masked with asterisks or other special characters, similar to the technique used when handling passwords and PINs.
- (17) Adequate internal control procedures must be employed to ensure the proper monitoring of authorized and unauthorized access to SSN and other PII data.

APPENDIX 2

OFFICE OF THE FEDERAL REGISTRAR SYSTEM OF RECORDS NOTICE (SORN) TEMPLATE

[Name of the Agency]

Privacy Act of 1974; System of Records

AGENCY: [agency name and, if applicable, agency component]

ACTION: Notice of [New/Altered/Re-established] Privacy Act System of Records

SUMMARY: [a plain language description of the system]

DATES: [the effective date of the notice]

ADDRESSES: [instructions for submitting comments on the system, including an e-mail address or a website where comments can be submitted electronically]

FOR FURTHER INFORMATION CONTACT: [instructions for submitting general questions about the system]

SUPPLEMENTARY INFORMATION: [background information about the proposal]

SYSTEM NAME AND NUMBER: [name and number of the system]

SYSTEM LOCATION: [physical address(es) where the system is located]

AUTHORITY FOR CONDUCTING THE MATCHING PROGRAM: [the specific legal authorities that authorize the maintenance of the system]

PURPOSE(S): [a plain-language description of the agency's purpose(s) for maintaining the system]

CATEGORIES OF INDIVIDUALS: [the categories of individuals about whom records are maintained in the system]

CATEGORIES OF RECORDS: [the categories of records maintained in the system, and if practicable, the specific data elements]

RECORD SOURCE CATEGORIES: [the categories of sources of records in the system]

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: [each routine use of the records contained in the system, including the categories of uses and the purposes of such use]

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: [the policies and practices of the agency regarding the storage of records]

POLICIES AND PRACTICES FOR RETRIEVABILITY OF RECORDS: [the policies and practices of the agency regarding retrievability of the records]

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: [the policies and practices of the agency regarding retention and disposal of records]

PHYSICAL, PROCEDURAL, AND ADMINISTRATIVE SAFEGUARDS: [a description of the physical, procedural, and administrative safeguards to which the system is subject]

SYSTEM MANAGER(S): [the name, title, business address, and contact information of the agency official(s) who is responsible for the system]

RECORDS ACCESS PROCEDURES: [the agency procedures whereby an individual can be notified at his/her request how he/she can gain access to any record pertaining to him/her in the system]

NOTIFICATION PROCEDURE: [the agency procedures whereby an individual can be notified at his/her request if the system contains a record pertaining to him/her]

CONTESTING RECORD PROCEDURES: [the agency procedures whereby an individual can be notified at his/her request how he/she can contest the content of any record pertaining to him/her in the system]

EXEMPTIONS PROMULGATED FOR THE SYSTEM: [any Privacy Act exemptions promulgated for the system]

APPENDIX 3

OFFICE OF THE FEDERAL REGISTRAR MATCHING ACTIVITIES NOTICE TEMPLATE

OMB requires the FCC and Federal agencies to publish all matching notices in the Federal Register using the format provided below. Agencies are to use the language section headings in the template and replace the language in brackets with the appropriate agency language.¹

Federal Communications Commission

Privacy Act of 1974; Matching Program

AGENCY: Federal Communications Commission (FCC)

ACTION: Notice of [New/Altered/Re-established] Matching Program

SUMMARY: [a plain language description of the matching program]

DATES: [the beginning and ending dates of the matching program (including whether the program is one time or continuing, and about the possibility of a one-year renewal by the DIB)]

ADDRESSES: [instructions for submitting comments on the matching program, including an e-mail address or a website where comments can be submitted electronically]

FOR FUTHER INFORMATION CONTACT: [instructions for submitting general questions about the matching program]

SUPPLEMENTARY INFORMAITON: [background information about the proposal]

PARTICIPATING AGENCIES: [the name of the participating agency or agencies, including any non-Federal agencies]

AUTHORITY FOR CONDUCTING THE MATCHING PROGRAM: [the specific legal authorities for conducting the matching program]

PURPOSE(S): [a plain-language description of the agency's purpose(s) for conducting the matching program]

CATEGORIES OF INDIVIDUALS: [the categories of individuals whose information is involved in the matching program]

CATEGORIES OF RECORDS: [the categories of records involved in the matching program and the specific data elements that are matched]

SYSTEM(S) OF RECORDS: [the names of all relevant system(s) of records and a citation of the SORN(s)]

¹ OMB Circular A-108 (2016), "Appendix III," at 40.

APPENDIX 4

MATCHING ACTIVITIES CHECKLIST

OMD asks each FCC Bureau and Office and OMD Division to complete this annual checklist for the FCC Data Integrity Board's computer matching review, as required under 5 U.S.C. 552a(o) of the *Privacy Act of 1974*, as amended and the *Computer Matching and Privacy Protection Act of 1988* (Public Law (Pub. L.) 100-503) ("CMPPA"). "Computer matching review" is an exchange of records containing PII between Federal agencies and between Federal and non-Federal agencies. For example, former FCC employee's debts are matched against the IRS Offset Program to collect delinquent debts owed by former FCC employees by withholding all or part of any tax refunds.

1. Bureau/Office/OMD Division (B/O/D): Consumer and Governmental Affairs Bureau (CGB)
2. Does your B/O/D maintain any information systems, databases, and/or paper files ("systems") that collect, store, and use information about individuals (*i.e.*, personally identifiable information or PII)? (Please mark with X)

Yes [] No []

If "yes," would you please list these systems that contain PII and indicate whether each system is covered by a System of Records Notice (SORN) and/or a Privacy Impact Assessment (PIA):

System(s)	SORN (Y/N)	PIA (Y/N)

3. Is your B/O/D engaged in any "matching activities" (*i.e.*, exchange of records containing PII between your B/O/D and an outside Federal or non-Federal agency) as provided for in the *Computer Matching and Privacy Protection Act of 1988* ("CMPPA"): (Please mark with X)

Yes [] No []

If your B/O will perform no matching activities that involve PII in FY 2015, please go to Question 13 on page 6.

4. If your B/O has been a participant in any matching activities in FY 2015, does the system of records notice (SORN) that covers the PII that is being matched include the appropriate routine use(s) (*i.e.*, third party disclosure) to cover the matching activity(s)?
(Please mark with X)

Yes [] No []

Matching Activities (Please also indicate whether your B/O/D is the source for the PII or the agency matching the PII in each matching activity)	Publication Date for Routine Use(s)	Federal Register Notice(s)

No, please provide an explanation here or attach the explanation at the end of this checklist:

5. Has your B/O/D rejected any proposed matching agreements?
(Please mark with X)

Yes [] No []

Rejected Proposed Matching Agreement Activities (Please also indicate whether your B/O/D was to be the source for the PII or the agency matching the PII in each rejected matching activity)

6. Does your B/O/D have a written agreement with the other Federal or non-Federal agency with which you are engaged in the matching activity that includes safeguards to cover the PII that is being matched, as required under OMB Matching Guidelines, Circular A-130, Appendix I, at 5(b)?
(Please mark with X)

Yes [] No []

If No, please provide the reason and date when the agreement(s) will be exchanged:

Reason(s) for why a written agreement has not yet be exchanged:	Date

7. Has your B/O/D had any violations of your matching agreements?
(Please mark with X)

Yes [] No []

Matching Agreement Violations (Please also indicate whether your B/O/D was the source for the PII or the agency matching the PII in each matching agreement violation)

8. Has your B/O/D been subject to any litigation based on inaccurate data in any matching agreements?
(Please mark with X)

Yes [] No []

<p style="text-align: center;">Matching Agreement Litigation (Please also indicate whether your B/O/D was the source for the PII or the agency matching the PII in each matching agreement violation)</p>

9. What are the estimated numbers of individuals whose records will be included in your B/O/D's matching activities, in each of the following categories?

Categories of Individuals in B/O/D Matching Activities	Estimated Number of Individuals
Benefit Records	
Personnel/employment Records	
Indebtedness/Accounts Receivable Records	
Provider Records	
Other Record Types	

- 10a. If your B/O/D has contractors participating in any matching agreements (*e.g.*, IT staff), do you have proper controls in place as required by Federal privacy statutes under and OMB regulation: ¹
(Please mark with X)

Yes [] No []

Contracts Containing Privacy Provisions for Contractors Engaged in Matching Agreements	Dates

- 10b. If there is no language covering the contractors who participate in any matching agreements, please provide an estimated date for when the new contract or contract revisions will be signed and assurances that contractors will not participate until that time.

Contract or Revisions covering Contractors Participating in Matching Agreements	Dates

¹ See *Final Guidance for Conducting Matching Programs*, Office of Management and Budget (54 FR 25819) June 19, 1989; Public Law 100-503, *Computer Matching and Privacy Protection Act of 1988*; *Computer Matching and Privacy Protection Act of 1988*, 5 U.S.C.552a, as amended; and *Guidance for Conducting Matching Programs*, Office of Management and Budget (47 FR 21656-21658) May 19, 1982, at 5(g).

11. Have you performed a cost/benefit analysis for any of your B/O/D's computer matching activities, pursuant to 5 U.S.C. §§ 552a(o) and 552a(u)(4)(A) of the *Privacy Act of 1974*, as amended?
(Please mark with X)

Yes [] No []

Matching Activity	Agreement Date

12. If your B/O/D is required to provide estimated cost/benefit figures for your B/O/D's matching activities—please attached the estimate(s) to this checklist.

13. Has you B/O/D engaged in any other types of data sharing or data matching agreements and activities with external organizations without any formal procedural arrangements for such activities?
(Please mark with X)

Yes [] No [X]

Other Types of Data Sharing and/or Matching Activities	Agreement Date

Thank you for your help.

Please sign and date this checklist for your B/O/D:

Signature of Completing Official and Office Telephone Number and Date

Senior Agency Official for Privacy (SAOP)

APPENDIX 5

FCC WEBSITE PRIVACY POSTING REQUIREMENTS¹

- (A) Policy. OMB regulations require the FCC to maintain a central resource page on the Commission's principle website at www.fcc.gov that is dedicated to its privacy program. A link to this page must be provided on any major entry points on the Commission's website.
- (B) Website Postings. At a minimum, the Commission is required to include the following materials on the agency's privacy program webpages:

(1) **System of Records Notices (SORNs):**

The FCC provides a SORN roster that includes the number of each SORN with a link to a copy of the official version that was published in the *Federal Register* (FR), the title of the SORN, and its FR publication date.

The link to the SORN roster is at:

<https://www.fcc.gov/general/privacy-act-information#systems>

(2) **Privacy Impact Assessments (PIAs):**

The Commission provides a PIA roster and a link at:

<https://www.fcc.gov/general/privacy-act-information#pia>. The PIA roster includes a link to each PIA.

(3) **Privacy Threshold Analyses (PTAs):**

The Commission also provides a PTA roster and a link at:

<https://www.fcc.gov/general/privacy-act-information#pia>. This PTA roster includes a link to each PTA.

(4) **Matching Notices and Agreements:**

The FCC lists and provides a link to a roster of all active matching notices and agreements in which the Commission is a participant, as required under section 8 of OMB Circular A-108.

(5) **Exemptions to the Privacy Act:**

The FCC lists all Privacy Act exemptions claimed for the Commission's systems of records and provides a link to the final rules published in the *Federal Register* that promulgate each exemption, as required under section 11 of OMB Circular A-108.

¹ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 15, "Agency Website Posting," at 30 - 31.

The list of these SORNs and their exemptions may also be found in Chapter 5 of the FCC Privacy Act Manual.

(6) Privacy Act Implementation Rules:

The FCC provides a list and link to all Privacy Act implementation rules promulgated pursuant to 5 U.S.C. 552a(f) of the Privacy Act, as required under section 10 of OMB Circular A-108.

- (a) The Commission's policies and procedures for notification, records access, contesting records, and correction of information contained in a system of records maintained by the Commission are found in Chapter 4 of the FCC Privacy Act Manual and under 47 CFR §§ 0.554 – 0.561 of FCC Rules.
- (b) The Commission's Freedom of Information Act/Privacy Act (FOIA/PA) search fees and related information are found at:
<https://www.fcc.gov/reports-research/guides/how-file-foia-request>

(7) Publicly Available FCC Reports on Privacy:

The FCC provides a roster and a link to all publicly available Commission reports on privacy.

Note: OMB does not require the FCC to include the agency's FISMA reports or reports provided to OMB and Congress pursuant to 5 U.S.C. 552a(r) of the Privacy Act.

(8) Instructions on Submitting a Privacy Act Request:

The FCC provides a link:
<https://www.fcc.gov/reports-research/guides/how-file-foia-request> for individuals to use to request access to or amendment of their records, which are contained in a system of records that the Commission maintains, as required under 5 U.S.C. 552a(d) of the Privacy Act.

(9) Contact Information for Submitting a Privacy Question or Complaint:

The FCC provides a link: <https://www.fcc.gov/general/privacy-act-information> to use to contact the Commission's privacy staff with their privacy questions and/or complaints.

(10) Identity of the Senior Agency Official for Privacy (SAOP):

The FCC provides the name and contact information of the SAOP for his/her office at:

APPENDIX 6

ADAPTED PRIVACY IMPACT ASSESSMENT (PIA) TEMPLATE¹

Section 1.0 – Specific purpose of the agency’s use of a third-party website or application:

- 1.1 What is the specific purpose of the agency’s use of the third-party website or application and how does that use fit with the agency’s broader mission?
- 1.2 Is the agency’s use of the third-party website or application consistent with all applicable laws, regulations, and policies?

Section 2.0 – Any PII that is likely to become available to the agency through the use of the third-party website or application:

- 2.1 What PII will be made available to the agency?
- 2.2 What are the sources of the PII?
- 2.3 Do the agency’s activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

Section 3.0 – The agency’s intended or expected use of the PII:

- 3.1 Generally, how will the agency use the PII described in Section 2.0?
- 3.2 Provide specific examples of the types of uses to which PII may be subject.

Section 4.0 – Sharing or Disclosure of PII:

- 4.1 With what entities or persons inside and/or outside the agency will the PII be shared, and for what purpose(s) will the PII be disclosed?
- 4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

Section 5.0 – Maintenance and retention of PII:

- 5.1 How will the agency maintain the PII, and for how long?
- 5.2 Was the retention period established to minimize risk?

Section 6.0 – How the agency will secure PII:

- 6.1 Will the agency’s privacy and security officials coordinate to develop methods of securing PII?

¹ OMB notes that agencies should use this model Adapted PIA template a general resource as an illustration, and that agencies should tailor their PIAs to fit their specific needs and uses. OMB also requests that agencies update the PIA template, as necessary to fit future requirements, as appropriate. *see* OMB Memorandum for CIOs, Dec. 29, 2011, at 5.

Section 7.0 – Identification and mitigation of other privacy risks:

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

Section 8.0 – Creation or modification of a system of records:

8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

DATES: [the effective date of the notice]

ADDRESSES: [instructions for submitting comments on the system, including an e-mail address or a website where comments can be submitted electronically]

FOR FUTURE INFORMATION CONTACT: [instructions for submitting general questions about the system]

SUPPLEMENTARY INFORMATION: [background information about the proposal]

SYSTEM NAME AND NUMBER: [name and number of the system]

SYSTEM LOCATION: [physical address(es) where the system is located]

AUTHORITY FOR CONDUCTING THE MATCHING PROGRAM: [the specific legal authorities that authorize the maintenance of the system]

PURPOSE(S): [a plain-language description of the agency's purpose(s) for maintaining the system]

CATEGORIES OF INDIVIDUALS: [the categories of individuals about whom records are maintained in the system]

CATEGORIES OF RECORDS: [the categories of records maintained in the system, and if practicable, the specific data elements]

RECORD SOURCE CATEGORIES: [the categories of sources of records in the system]

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: [each routine use of the records contained in the system, including the categories of uses and the purposes of such use]

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: [the policies and practices of the agency regarding the storage of records]

POLICIES AND PRACTICES FOR RETRIEVABILITY OF RECORDS: [the policies and practices of the agency regarding retrievability of the records]

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: [the policies and practices of the agency regarding retention and disposal of records]

PHYSICAL, PROCEDURAL, AND ADMINISTRATIVE SAFEGUARDS: [a description of the physical, procedural, and administrative safeguards to which the system is subject]

SYSTEM MANAGER(S): [the name, title, business address, and contact information of the agency official(s) who is responsible for the system]

RECORDS ACCESS PROCEDURES: [the agency procedures whereby an individual can be notified at his/her request how he/she can gain access to any record pertaining to him/her in the system]

NOTIFICATION PROCEDURE: [the agency procedures whereby an individual can be notified at his/her request if the system contains a record pertaining to him/her]

CONTESTING RECORD PROCEDURES: [the agency procedures whereby an individual can be notified at his/her request how he/she can contest the content of any record pertaining to him/her in the system]

EXEMPTIONS PROMULGATED FOR THE SYSTEM: [any Privacy Act exemptions promulgated for the system]

APPENDIX 7

OMB GUIDANCE ON THE ADAPTED PRIVACY IMPACT ASSESSMENT (PIA) TEMPLATE¹

Section 1.0 – Specific purpose of the agency’s use of a third-party website or application:

- 1.1 What is the specific purpose of the agency’s use of the third-party website or application and how does that use fit with the agency’s broader mission?
- The Commission should use plain language to disclose the purpose(s) for its use of the third party websites or applications.
 - Since the Commission’s purpose(s) for using different third party websites and applications may differ, the Commission should explain in the adapted PIA its purpose(s) in the context of its specific mission, *e.g.*, to facilitate public dialogue; to provide information about or from the FCC; and/or to improve customer service, on each website and application, unless, of course, these websites and applications have such similar functions, which a single, adapted PIA can cover.
- 1.2 Is the agency’s use of the third-party website or application consistent with all applicable laws, regulations, and policies?
- The Commission should make clear that it will comply with all applicable laws, regulations, and policies, in particular those pertaining to privacy, accessibility, information security, and records management.
 - Employees and contractors should work with the SAOP and privacy staff to ensure that the Commission’s use of third party websites and applications remains in compliance.

Section 2.0 – Any PII that is likely to become available to the agency through the use of the third-party website or application:

- 2.1 What PII will be made available to the agency?
- Registration: Since many third party websites or applications requests PII at the time of registration, the FCC should make clear whether the Commission will have access to this PII and whether users can take steps to limit the Commission’s access.
 - Submission:

¹ OMB notes that agencies should use this model Adapted PIA template a general resource as an illustration, and that agencies should tailor their PIAs to fit their specific needs and uses. OMB also requests that agencies update the PIA template, as necessary to fit future requirements, as appropriate. See Kevin Neyland, OIRA, OMB Memorandum for CIOs, *Model PIA Assessment for Agency Use of Third Party Websites and Applications*, Dec. 29, 2011.

- (a) An individual can make PII available to the Commission when he/she provides, submits, communicates, links, posts, or associates PII while using the third party website or application, *i.e.*, “friend-ing,” “follow-ing,” “lik-ing,” joining a group, “becoming a “fan,” and comparable functions.
 - (b) Individuals may provide their PII during their sign-up/log-on transactions or during subsequent interactions.
 - (c) If these individuals post their PII in the website’s public area or send it to the Commission in connection with the transaction of business, this may make their PII Federal records.
- Association:
 - (a) Even when individuals do not actively post or submit information, they can potentially make PII available to the Commission by “associating” themselves with the websites or applications, *i.e.*, “friend-ing,” “follow-ing,” “lik-ing,” joining a group, “becoming a “fan,” and comparable functions.
 - (b) These activities may make the user’s PII more widely available than is immediately obvious to the user, e.g., there may be a link on the third party website or application that is then linked to a different third party website or application without the user’s knowledge or consent.
- Accounts:
 - (a) Even individuals who do not have an account with a third party website or application may make PII available to the Commission if certain functions of the website application are available to individuals without an account by commenting on images or video or otherwise submitting information.
 - (b) The FCC should state clearly whether or not the Commission will have access to this PII, and whether users can take steps to limit the Commission’s access.

2.2 What are the sources of the PII?

- Users may be required to submit PII to the third party website or application when registering, which the website or application may collect and maintain.
- This PII may also be available to the Commission in many circumstances, *e.g.*, if there is some link or connection for the Commission via this third party website or application, the Commission may have access to an individual’s PII when he/she is engaged in transactions on the website or application or if he/she communicates with others.
- It is important to recognize that the Commission may gain access to information in ways that are not obvious to users, e.g., when individuals communicate with others if this activity is somehow connected to the FCC’s webpage or profile.

2.3 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

- Refer to the April 10, 2010 OMB Memorandum, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, to determine whether the PRA will apply – and briefly explain the determination.

Section 3.0 – The agency's intended or expected use of the PII:

3.1 Generally, how will the agency use the PII described in Section 2.0?

- A key decision for the Commission in the development of a PIA is that once it has identified the PII that is likely to be made available through the use of a third party website or application, it must then determine whether it will use this PII for any purpose.
- The Commission must address the potential uses of any PII that is likely to become available to it. In the event that the Commission decides to change these uses, then the PIA may need to be revised.
- When no PII will be used from several websites or applications or from multiple pages of a single website, the Commission may use a single, comprehensive PIA to cover multiple websites or applications, provided that the privacy, security, and retention issues are sufficiently comparable.
- When the Commission will use PII, then we must consider both current uses of the PII that are made available through third party websites or applications and also the potential future uses of the PII both:
 - (a) to provide the public with notice of the Commission's future actions; and
 - (b) to prepare us to identify and address the full range of privacy risks.
- The Commission should consider all the potential uses of the PII and all the alternative approaches that may mitigate the risks in these various uses, and then provide users with the (safe and secure) option of using the FCC official website in lieu of a third party website.

3.2 Provide specific examples of the types of uses to which PII may be subject.

These are OMB's examples of the kinds of issues that a PIA should address:

- Public interaction/open government activities, *i.e.*, using contests, surveys, and message boards for public comments on the Commission's activities.
- Recruitment and/or employee outreach, *i.e.*, using third party websites or applications to recruit and hire from the widest possible pool of candidates or to inform or to receive feedback from current employees.

- Participating in agency programs or systems, *i.e.*, using third party websites or applications to facilitate access to FCC programs or systems. Consideration of such uses should address whether this use will result in PII being combined, matched, or otherwise used in concert with PII that is already maintained by the Commission.
- Web measurement and/or customization, *i.e.*, using third party websites or applications to conduct measurement and analysis of web usage, or to customize the user's experience, per the guidance provided in OMB Memorandum M-22-10, *Guidance for Online Use of Web Measurement and Customization Technologies* (June 25, 2010).

Section 4.0 – Sharing or Disclosure of PII:

- 4.1 With what entities or persons inside and/or outside the agency will the PII be shared, and for what purpose(s) will the PII be disclosed?
 - The Commission should describe all entities to which any PII may be disclosed, and explain the specific authority for each type of disclosure.
 - The Commission should explain how any disclosure will comply with applicable laws, regulations, and policies.
 - The Commission should describe any expected dissemination activities and discuss any circumstances in which PII is like to be disclosed through the FCC's activities.
- 4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?
 - The Commission should describe the safeguards that are established to ensure that the PII is used only as permitted by law.
 - The Commission should describe the safeguards that are established to ensure that the FCC's uses of PII do not exceed or differ from the precise uses described in the PIA.

Section 5.0 – Maintenance and retention of PII:

- 5.1 How will the agency maintain the PII, and for how long?
 - The Commission should describe how it will maintain the PII and precisely how long the PII will be retained.
 - In addition to inclusion in a system of records, the Commission should describe the safeguards that are established to ensure that the FCC's other uses of PII, *e.g.*, copying individual comments into a document or database, etc., do not exceed or differ from the precise uses described in the PIA.

5.2 Was the retention period established to minimize risk?

- The Commission should establish the retention standards and requirements for any PII that it will maintain, in compliance with applicable laws, regulations, and policies, *e.g.*, the applicable NARA general record schedule.
- The Commission should describe these standards and explain why they were adopted.

Section 6.0 – How the agency will secure PII:

6.1 Will the agency's privacy and security officials coordinate to develop methods of securing PII?

- The Commission should consult the government-wide policies that pertain to information security, *e.g.*, NIST, OMB, and the CIO Council.
- The CIO Council also recommends that the Commission's privacy, security, and legal divisions: SAOP, CISO, CSO, CIO, and OGC *et al.*, work together to protect PII.
- The FCC should use plain language to describe:
 - (a) The basic methods that the Commission will use to secure any PII that it uses or maintains;
 - (b) How the Commission will limit access to the PII;
 - (c) Whether and how the Commission will encrypt or use other technical methods to secure the PII; and
 - (d) What steps the Commission will take to reduce the volume of PII to the minimum necessary to accomplish its purposes.

Section 7.0 – Identification and mitigation of other privacy risks:

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

- Disclosure of PII by users:
 - (a) The Commission may choose to delete or hide a user's comments or other interactions, *e.g.*, sharing or disclosing information containing PII, to mitigate the potential risks that these interactions with the FCC or others on a third party website potentially expose their PII to other users or any individuals with access to the site.
 - (b) The Commission should include in the privacy training guidance instruction to employees and contractors about not soliciting sensitive information when interacting with users on behalf of the FCC on these third party websites.

- (c) The Commission, when possible, should also provide appropriate notice to users on the third party website itself, warning users to avoid sharing or disclosing sensitive PII when interacting with the FCC on the site, as such sharing or disclosing PII may make this information available to other users or other parties with access to the site.
- Third party advertising and tracking:
 - (a) A third party website may display advertising or other special communications on behalf of other businesses or organizations. If the user clicks on the advertising or accesses the communications, this may allow the website operator to share the user's PII with the advertiser.
 - (b) The user's actions (*e.g.*, clicking on this advertising or reading communications) may also initiate tracking technology (*e.g.*, "cookies," "web bugs," or "beacons"), enabling the website operator or advertiser to create or develop a history or profile of the user's activities.
 - (c) The Commission should provide appropriate notice to users on the third party website itself, warning them about the privacy issues raised by such advertising and tracking technology.
- Spam, unsolicited communications, spyware, and other threats:
 - (a) The Commission should warn users that they receive spam or other unsolicited or fraudulent communications from a third party as a result of their interactions with the Commission on the website.
 - (b) The Commission should warn users to be wary of responding to such communications, particularly those that may solicit the user's PII.
 - (c) The Commission should warn users to avoid accepting or viewing unknown or unsolicited links, applications, or other content that may be sent or forwarded, which may contain unwanted tracking technology, computer viruses, or other malicious payloads that can pose a variety of risks to the user.
 - (d) The Commission's warning notice about these potential privacy risks and vulnerabilities, should, when feasible, be placed on the third party website itself.
- Accounts or pages that misrepresent agency authority or affiliation:
 - (a) Certain accounts or pages on a third party website may not be official authorized by, or affiliated with, the Commission, even if they use official insignia or otherwise appear to represent the FCC or the Federal Government.
 - (b) Interacting with such unauthorized accounts or pages may expose users to many of privacy or security risks of these other accounts or website pages.
 - (c) The Commission should make an effort to label or identify its account page in what that help users distinguish it from unauthorized accounts or pages.

- (d) The Commission should also, where appropriate, inform the website operator about any unofficial accounts or pages purporting to represent the FCC, seek their removal, and warn users about such accounts or pages.
 - (e) The Commission should explain that the FCC does not own, operate, or control the host website and should provide users with a direct link to the FCC's official website.
- External links and embedded third party applications:
 - (a) If the Commission posts a link that leads to a third party website or other location that is not part of an official government domain, the Commission should provide notice to the user to explain that the users are being directed to a nongovernment website that may have different privacy policies (and risks) from those of the official FCC website.
 - (b) If the commission incorporates or embeds a third party website or application, separate from any applications that may be incorporated or embedded by the website operator itself, the Commission should disclose and explain the nature or extent, if any, of the third party's involvement in the FCC's use of the application(s).
 - (c) The Commission should also describe the use of these application(s) in the Commission's own privacy policy.
- Monitoring future requirements and future technology:
 - (a) The Commission should establish and maintain procedures to identify, evaluate, and address any additional privacy requirements that may result from new statutes, regulations, or policies.
 - (b) The Commission should also monitor new technologies, consider new risks that may emerge, and look for new approaches to protect privacy.
- Monitoring the third party websites privacy policies:
 - (a) The FCC should make clear that the Commission has examined the third party website's privacy policy and have determined that the website is appropriate for the FCC's use.
 - (b) The Commission should monitor any changes in the third party's privacy policies and periodically reassess the risks and vulnerabilities for the FCC's continued use of the website.

Section 8.0 – Creation or modification of a system of records:

- 8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?
- The Commission should determine whether its use of the third party website or application will involve records that are subject to the requirements of the Privacy Act, *i.e.*, will a system of records need to be created or updated/revised to cover the records.

APPENDIX 8

SENIOR AGENCY OFFICIAL FOR PRIVACY ANNUAL FISMA PRIVACY REPORT

- (A) Policy. As required by OMB Circular A-108, the FCC's Senior Agency Official for Privacy (SAOP) shall ensure that the Commission has procedures in place to perform the following Privacy Act reviews on an on-going basis. The SAOP has determined that the FCC will perform these reviews in cooperation with the Bureaus, Offices, and OMD Divisions (B/O/Ds) on an annual basis. This annual review will be done:

- (1) To ensure that the Commission can confirm that it continues to maintain the safety and security of the personally identifiable information (PII) that it collects, uses, and stores; and
- (2) To comply with the requirements of the Privacy Act, OMB policies and guidelines, and as part of the SAOP's annual Privacy Report to OMB as required by the Federal Information Security and Management Act (FISMA).¹

- (B) Bureau and Office Reviews. The FCC's SAOP and privacy staff will review these privacy requirements with knowledgeable staff (employees and contractors) from each Bureau, Office, and OMD Division.

- (1) **Systems of Records Notices (SORNs):**²

The review and evaluation of each SORN maintained by a B/O/D (where applicable) to ensure that the scope of the system remains appropriate; that the system does not include any information about an individual that is not relevant and necessary to accomplish a purpose required by statute or executive order; that the SORN accurately describes the system; and that the SORN includes the information required by section 6(b) of OMB Circular A-108.

This review and evaluation will also determine whether there are new systems of records that need to be added or systems of records that should be consolidated or eliminated.

When changes to an existing SORN are needed, or a new SORN created, the privacy staff will work with the B/O to revise the SORN (as appropriate) and to publish it in the *Federal Register*. If the changes are significant, the Commission will submit the proposed altered SORN in advance to OMB and Congress for their review and sign-off, as required by section 6(k) of OMB Circular A-108.

- (2) **Routine Uses:**³

¹ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 27.

² OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 27-28.

³ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 28.

The review and evaluation of all routine uses associated with each SORN maintained by a B/O/D (where applicable) to ensure that the routine uses remain appropriate and that the recipient's use of these records continues to be compatible with the purpose(s) for which the information was collected, as required by section 6(k) of OMB Circular A-108.

This review and evaluation will also determine whether there are new routine uses that should be added to a system of records or routine uses that should be eliminated.

(3) **Privacy Act Exemptions:**⁴

The review and evaluation of each system of records maintained by a B/O/D (where applicable) for which the Commission has promulgated exemption rules pursuant to 5 U.S.C. 552a(j) and (a)(k) of the Privacy Act, in order to ensure that such exemptions remain appropriate and necessary and that no changes to the exemption are needed, as required by Section 11 of OMB Circular A-108.

This review and evaluation will also determine whether there are systems of records that the Commission should now exempt or systems of records that should no longer be exempt.

(4) **Social Security Numbers (SSNs):**⁵

The review and evaluation of s B/O/D's collection and use of SSNs (where applicable) to ensure that all the collections and uses of SSNs are specifically authorized and necessary, to eliminate all unauthorized or unnecessary collections and uses, and to explore alternatives to the collection and use of SSNs, where practicable.

(5) **Recordkeeping:**⁶

The review and evaluation of a B/O/D's recordkeeping and disposal policies and practices (where applicable) in order to ensure compliance with the Privacy Act and the appropriate records retention schedules approved by the National Archives and Records Administration (NARA).

This review and evaluation will also determine whether there are SORNs that required changes to their NARA records retention and disposal schedules.

- (C) Agency-wide Reviews: The FCC's SAOP and privacy staff will review these agency-wider privacy requirements with knowledgeable staff (employees and contractors) from the appropriate Bureau, Office, and OMD Division.

⁴ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 28.

⁵ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 28.

⁶ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 28.

(1) **Contracts:**⁷

The review and evaluation of a representative sample of the Commission's contracts that provide for the operation of a system of records on behalf of the FCC to accomplish a Commission function, in order to ensure that the language of each contract makes the provision of the Privacy Act and appropriate OMB guidance binding and enforceable on the contractor and its employees, as required by section 6(j) of OMB Circular A-108.

(2) **Privacy Training:**⁸

The review and evaluation of the FCC's privacy training practices at all levels, including initial, annual, and specialized training for employees and contractors, in order to ensure that all Commission personnel are familiar with the requirements of the Privacy Act, OMB guidance, and the FCC's implementing regulations and policies, and any job-specific requirements, *e.g.*, specialized privacy training for employees and contractors whose job duties and responsibilities require their access to and use of PII, which will also include consultation with the appropriate B/O/D supervisors/managers where appropriate.

(3) **Violations:**⁹

The review and evaluation of any confirmed or reported violations of the Privacy Act at the Commission in order to determine whether a problem occurred, ascertain the extent of the problem, and find the most effective way to address the problem and to prevent its recurrence.

(D) Certification:

Upon completion of these Privacy Act reviews, the B/O/D representatives and the privacy staff will sign their respective review document's certification.

The SAOP will conduct a review of each B/O/D's review document. The SAOP may consult the B/O/Ds with any questions, comments, and/or concerns. The SAOP will also sign each review document certifying to his/her agreement with the document's findings and its compliance with the FCC's privacy regulations, Privacy Act, OMB regulations, and FISMA requirements.

⁷ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 27-28.

⁸ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 27-28.

⁹ OMB Circular A-108 (2015 draft), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, Section 12, "Privacy Act Reviews," at 27-28.

APPENDIX 9

BUREAU, OFFICE, and OMD DIVISION FISMA PRIVACY ACTIVITIES REPORTING QUESTIONNAIRE

Bureau/Office/Division (B/O/D):

B/O/D Participants:

FY 2016 FISMA Review Questions	FCC owned systems	Contract or owned systems
1. How many information systems, databases, and paper files does your Bureau/Office maintain that contain personally identifiable information (PII), <i>i.e.</i> , information about individuals?		
2. How many of these systems that contain PII have a Privacy Impact Assessment (PIA) as required by OMB Memorandum M-03-22?		
3. How many of these systems that contain PII have a System of Records Notice (SORN) as required by the Privacy Act of 1974 (5 U.S.C. 552a)?		
4. Did your Bureau/Office receive any written complaints concerning FOIA/Privacy requests this year?		
4.a. If so, how many written complaints, and for what reason(s)?		
5. For Bureaus/Offices with SORNs - have you conducted a mandatory annual review of the following:		
a. Section (m) Contracts (5 U.S.C. 552a(m)) that require contractors to abide by Federal privacy requirements as Federal workers do		
b. Records retention and disposal practices?		
c. Routine uses?		
d. Exemptions (where applicable) from the records notification, access, and contesting requirements of the Privacy Act (5 U.S.C. 552a(j) and a(k))		
e. Matching programs (where applicable)?		
e.1. If you conducted any matching programs, how many did you conduct?		
f. Privacy training for the employees and contractors who have access to the PII as part of their job duties?		
g. Privacy violations, <i>i.e.</i> , inadvertent disclosure of the PII in your system(s)?		
h. Remedial actions (where applicable) for any privacy violations?		
i. System of records notices (SORN) – did you review the SORNs for other possible changes or deletions (besides changes to the SORN components listed above)?		
j. Forms containing PII that require a Privacy Statement as required by subsection (e)(3) of the Privacy Act (5 U.S.C. 552a)?		
k. Systems that contain PII that require a Privacy Impact Assessment (PIA) and/or updates?		
l. Data mining activities that were conducted?		
l.1. If so, how many data mining activities?		

2. What is your Bureau/Office/Division doing to eliminate the unnecessary use(s) of Social Security Numbers?
(Please update the information (as applicable) that was submitted in last year's FISMA Report).

3. What is your Bureau/Office/Division doing to reduce its holdings of personally identifiable information (PII)?
Please update the information (as applicable) that was submitted in last year's FISMA Report).

Thank you for your help.

Please sign and date this FISMA Reporting Questionnaire for your B/O/D:

Signature of Completing Official and Office Telephone Number and Date

Senior Agency Official for Privacy (SAOP)