notice requirements. Accordingly, the predominant costs incurred by operators are the aforementioned labor costs. Similarly, FTC staff anticipates that covered entities already have in place the means to retain and store the records that must be kept under the Rule's safe harbor recordkeeping provisions, because they are likely to retain such records independent of the Rule. Accordingly, FTC staff estimates that the capital and non-labor costs associated with Rule compliance are *de minimis.*

Request for Comment

Pursuant to section 3506(c)(2)(A) of the PRA, the FTC invites comments on: (1) whether the disclosure and recordkeeping requirements are necessary, including whether the information will be practically useful; (2) the accuracy of our burden estimates, including whether the methodology and assumptions used are valid; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information.

For the FTC to consider a comment, we must receive it on or before November 29, 2024. Your comment, including your name and your state, will be placed on the public record of this proceeding, including the *https://www.regulations.gov* website.

You can file a comment online or on paper. Due to heightened security screening, postal mail addressed to the Commission will be subject to delay. We encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you file your comment on paper, write ''COPPA Rule: Paperwork Comment, FTC File No. P155408'' on your comment and on the envelope, and mail it to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC–5610 (Annex J), Washington, DC 20580.

Because your comment will become publicly available at *https://www.regulations.gov,* you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any ''trade secret or any commercial or financial information which . . . is privileged or confidential''—as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including, in particular, competitively sensitive information, such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must (1) be filed in paper form, (2) be clearly labeled ''Confidential,'' and (3) comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at *www.regulations.gov,* we cannot redact or remove your comment unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before November 29, 2024. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy.*

Josephine Liu,

Assistant General Counsel for Legal Counsel.

[FR Doc. 2024–22379 Filed 9–27–24; 8:45 am]

BILLING CODE 6750–01–P

FEDERAL TRADE COMMISSION

Privacy Act of 1974; System of Records

AGENCY: Federal Trade Commission (FTC).

ACTION: Notice of modified systems of records.

SUMMARY: The FTC is making technical revisions to several of the notices that it has published under the Privacy Act of 1974 to describe its systems of records. This action is intended to make these notices clearer, more accurate, and up-to-date.

DATES: These modified systems will be applicable on September 30, 2024.

FOR FURTHER INFORMATION CONTACT: G. Richard Gold, Attorney, Office of the General Counsel, FTC, 600 Pennsylvania Avenue NW, Washington, DC 20580, (202) 326–3355 or *rgold@ftc.gov.*

SUPPLEMENTARY INFORMATION: To inform the public, the FTC publishes in the **Federal Register** and posts on its website a ''system of records notice'' (SORN) for each system of records that the FTC currently maintains within the meaning of the Privacy Act of 1974, as amended, 5 U.S.C. 552a (''Privacy Act'' or ''Act''). See *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems.* The Privacy Act protects records about individuals in systems of records collected and maintained by Federal agencies. (A system is not a ''system of records'' under the Act unless the agency maintains and retrieves records in the system by the relevant individual's name or other personally assigned identifier.) Each Federal agency, including the FTC, must publish a SORN that describes the records maintained in each of its Privacy Act systems, including the categories of individuals that the records in the system are about where and how the agency maintains these records, and how individuals can find out whether an agency system contains any records about them or request access to their records, if any. The FTC, for example, maintains 39 systems of records under the Act. Some of these systems contain records about the FTC's own employees, such as personnel and payroll files. Other FTC systems contain records about members of the public, such as public comments, consumer complaints, or phone numbers submitted to the FTC's Do Not Call Registry.

The FTC's SORNs discussed in this notice apply only to the FTC's own Privacy Act record systems. They do not cover Privacy Act records that other Federal agencies may collect and maintain in their own systems. Likewise, the FTC's SORNs and the Privacy Act of 1974 do not cover personal records that private businesses or other non-FTC entities may collect, which may be covered by other privacy laws.

Based on a periodic review of its SORNs, the FTC is publishing these additional technical revisions, to ensure that the FTC's SORNs and Appendices remain clear, accurate, and up-to-date:

- First, the FTC is amending several SORNs to clarify or update information about the applicable records disposition schedules published or approved by the National Archives and Records Administration (NARA). These schedules determine how long agency records in each system should be retained and destroyed.
- Second, the FTC is amending multiple SORNs to make other technical changes (*e.g.,* updating the official title of the system manager, the authority for maintenance of the system, and the policies and practices for storage and record retention of records).
- Third, the FTC is republishing the full text of each of the above SORNs, incorporating the technical amendments, for the convenience of the reader and in accordance with OMB Circular A–108 (2016), which reorganized the format and content for SORNs published by Federal agencies.

The FTC is not substantively adding or amending any routine uses of its Privacy Act system records. Accordingly, the FTC is not required to provide prior public comment or notice to OMB or Congress for these technical amendments, which are final upon publication. See 5 U.S.C. 552a(e)(11) and 552a(r); OMB Circular A–108, supra.

A SORN-by-SORN summary, including a more detailed description of each SORN and how it is being amended, appears below, followed by the full text of the SORNs, as amended.

I. Law Enforcement Systems of Records

FTC–I–3 (Informal Advisory Opinion Requests and Response Files—FTC). This SORN covers the records of individuals who have requested informal advisory opinions from the FTC staff, and records of the responses to such requests. The Commission has updated the sections relating to the System Manager, Policies and Practices for Storage of Records, and Policies and Practices for Retrieval of Records.

FTC–I–5 (Matter Management System—FTC). This SORN covers the administrative database used by the FTC to track and report the history and status of FTC investigations and other agency matters, including names of employees or others assigned to or involved in such matters. The Commission has updated the sections relating to the System Manager and Policies, Purpose of the System, Categories of Records, Policies and Practices for Retrieval of Records, and Policies and Practices for Retention and Disposal of Records.

FTC–I–6 (Public Records—FTC). This SORN covers the FTC's system of public records, including comments submitted by consumers and others in rulemakings, workshops, or other FTC proceedings. The FTC makes these public records routinely available for public inspection and copying, including by posting copies of such records on the internet, as noted in section 4.9(b) of the FTC Rules of Practice, 16 CFR 4.9(b), and explained in the FTC's online privacy policy posted at *www.ftc.gov.* This SORN has been updated to add an additional System Manager, the website Manager, Office of Public Affairs, and to update Policies and Practices for Retrieval of Records, and Administrative, Technical, and Physical Safeguards.

FTC–I–7 (Office of Inspector General Files—FTC). This SORN covers records in the FTC's Office of Inspector General (OIG). The OIG maintains this system of records to carry out its responsibilities pursuant to the Inspector General Act, as amended. This system was last revised in 2009. Among other minor changes, this SORN has been updated under System Name, Purpose, Categories of Individuals Covered by the System, Categories of Records in the System, Record Source Categories, Policies and Practices for Storage of Records, Retention and Disposal of Records, and Administrative, Technical, and Physical Safeguards.

II. Federal Trade Commission Personnel Systems of Records

FTC–II–11 (Personnel Security, Identity Management & Access Control Records—FTC). This SORN covers security-related records for determining the eligibility of FTC employees or other authorized individuals (*e.g.,* on-site contractors) for access to FTC facilities and resources, as well as records related to granting and controlling such access. This SORN has been updated to add an additional System Manager, the Human Capital Management Office, and an additional Record Source Category to include the Defense Counterintelligence and Security Agency (DCSA).

IV. Correspondence Systems of Records

FTC–IV–1 (Consumer Information System—FTC). This SORN covers consumer complaints and information requests received from consumers, as well as identity theft complaints. Among other updates, the Commission has updated the sections relating to the System Manager, Policies and Practices for Storage of Records, and Policies and Practices for Retention and Disposal of Records.

FTC–IV–3 (National Do Not Call Registry—FTC). This SORN covers records of individuals who wish to be placed on the FTC's telemarketing do-not-call list. It also covers information collected from telemarketers, sellers, or agents who are required to comply with the list, but only to the extent, if any, that such telemarketers, sellers, or agents are also ''individuals'' within the meaning of the Privacy Act. The FTC is revising the sections on System Location, Practices for Retention and Disposal of Records, Record Access Procedures, and Contesting Record Procedures.

VII. Miscellaneous Systems of Records

FTC–VII–1 (Automated Library Management System—FTC). This SORN covers requests from FTC employees and other individuals to search for holdings in the FTC Library's collection. The Commission has updated the Categories of Individuals Covered by the System.

FTC–VII–6 (Matter Record Search System (MaRS)—FTC). This SORN covers legacy and current electronic data collections of FTC memoranda and other agency records that may be managed by and retrieved by the author's name or other personal identifiers. The FTC has revised the System Name, System Manager, and Administrative, Technical, and Physical Safeguards.

FTC Systems of Records Notices

In light of the updated SORN template set forth in the revised OMB Circular A–108 (2016), the FTC is reprinting the entire text of each amended SORN when necessary for the public's benefit, to read as follows:

I. Law Enforcement Systems of Records

* * * * *

SYSTEM NAME AND NUMBER:

Informal Advisory Opinion Request and Response Files—FTC (FTC–I–3).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Office of the Secretary, Records Management Division, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*

PURPOSE(S) OF THE SYSTEM:

To respond to requests for informal advisory opinions; to maintain records of such requests and the staff's responses; for use by staff in coordinating and preparing future advisory opinions and assuring the consistency of such opinions; to make records of such requests and staff responses available within the FTC for historical, legal research, investigational, and similar purposes (see FTC–VII–6, Document Management and Retrieval System—FTC); and also to make appropriate portions of such records available to the public (see FTC–I–6, Public Records—FTC).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Applicants for informal advisory opinions from FTC staff under § 1.1(b) of the Commission's Rules of Practice, 16 CFR 1.1(b). (Applicants for formal advisory opinions from the Commission under § 1.1(a) of the Rules of Practice, 16 CFR 1.1(a), are covered by FTC–I–1, Nonpublic Investigational and Other Nonpublic Legal Program Records—FTC.)

CATEGORIES OF RECORDS IN THE SYSTEM:

Name of author and documents written by that individual; names or other data about other individuals by which documents in the system are searched and retrieved; finding aids or document indexes. Records in this system may duplicate records included in other FTC systems of records. See, *e.g.,* FTC–I–1 (Nonpublic Investigational and Other Nonpublic Legal Program Records—FTC), FTC–I–6 (Public Records—FTC).

RECORD SOURCE CATEGORIES:

Individual proprietorship, corporation, or other business organization, counsel seeking or receiving a staff advisory opinion, and FTC employees.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system may be:

(1) Referred to appropriate federal or state agencies for advice, for law enforcement, or where law enforcement action may be warranted; and

(2) Disclosed on the FTC's public record under the FTC's Rules of Practice. See FTC–I–6, Public Records—FTC.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55541, 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The FTC maintains these records in electronic and non-electronic formats and media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are indexed by name of requesting party and subject matter of the opinion.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of under applicable schedules and procedures approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

For records other than those made public, access is restricted to agency personnel or contractors whose responsibilities require access. Paper records are maintained in lockable rooms or file cabinets. Access to electronic records is controlled by ''user ID'' and password combination and/or other appropriate electronic access or network controls (*e.g.,* firewalls). FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

73 FR 33591–33634 (June 12, 2008).

* * * * *

SYSTEM NAME AND NUMBER:

Matter Management System—FTC (FTC–I–5).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Office of the Secretary, Records Intake and Processing Division, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*

PURPOSE(S) OF THE SYSTEM:

This system, currently known within the FTC as Matter Management System 2 (MMS2), is used to record and track the status or occurrence of planned or actual actions and events that may arise in investigations, rulemakings, or other Commission matters, and to generate status or history reports on these actions, events, and matters for use by Commission management and staff, in combination, as needed, with matter-related data from other systems. Specific purposes of this system (FTC–I–5) include: to maintain records of employee work and Commission law enforcement activities; to make workload and budget determinations and personnel-related evaluations; to assist in investigative and adjudicative proceedings, enforcement actions, civil penalty proceedings, consideration of

compliance reports, issuance of cease and desist orders, advisory opinions, and other Commission matters and proceedings; to refer information compiled in system records to experts and consultants when considered appropriate by Commission staff; and to use those records to properly manage Commission resources.

This system includes a subsystem of records to record and keep track of the status of matters pending for a vote or other review or action before the full Commission (*i.e.,* the five Federal Trade Commissioners). The specific purposes of those records include: to process and control assignments made to individual Commissioners; to coordinate the consideration of and votes on appropriate issues; to assist Commissioners and staff in investigative, adjudicative and rulemaking proceedings, enforcement actions, civil penalty proceedings, consideration of compliance reports, issuance of complaints, negotiation of consent orders, issuance of cease and desist orders, advisory opinions, and other matters before the Commission; and to retain records of the matters before the Commission, the Commission's deliberations and decisions concerning those matters, and related documents.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Past and present Commission employees, and other participants or parties in Commission investigations, rulemaking, advisory, and law enforcement matters or proceedings. (Businesses, sole proprietorships, or corporations are not covered by this system.)

CATEGORIES OF RECORDS IN THE SYSTEM:

For records about past or present Commission employees: employee name; employee identification number; organization name and code; employee assignments to individual matters. For others: records related to investigatory, rulemaking, advisory opinion and other matters or proceedings, including matter name and associated matter number; matter status; alleged or potential law violation; and goods or services associated with the proceeding. The records also includes names and mailing addresses of civil investigative demand and subpoena recipients and names of deponents, as well as brief descriptions or summaries of planned or actual actions or events during an FTC investigation, rulemaking, court case, or other FTC matter or proceeding. The system also includes records of assignments, votes, circulations, or other activities or actions of the FTC's Commissioners on agency proceedings and matters.

RECORD SOURCE CATEGORIES:

Individual on whom the record is maintained and Commission staff associated with the matter.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system:

(1) May be made available or referred to federal, state, local or international government authorities for investigation, possible criminal prosecution, civil action, regulatory order or other law enforcement purpose; and

(2) May be disclosed on the FTC's public record under the FTC's Rules of Practice. See FTC–I–6, Public Records—FTC.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55541, 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

System records are primarily maintained and accessed electronically. The system can generate electronic or printed status or history reports.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by Commissioner, staff, or other individual name, employee identification number, respondent's or correspondent's name, company name, industry investigation title, and FTC matter number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with schedules and procedures issued or approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

For records other than those made public, access is restricted to agency personnel or contractors whose responsibilities require access. Access to nonpublic electronic records is controlled by ''user ID'' and password combination and/or other appropriate electronic access or network controls (*e.g.,* firewalls). FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Copies of records contained in this system that have been placed on the FTC public record are available upon request or from the FTC's website, where applicable. See FTC–I–6, Public Records—FTC. However, pursuant to 5 U.S.C. 552a(k)(2), records in this system, which reflect records that are contained in other systems of records that are designated as exempt, are exempt from the requirements of subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of 5 U.S.C. 552a. See § 4.13(m) of the FTC Rules of Practice, 16 CFR 4.13(m).

HISTORY:

73 FR 33591–33634 (June 12, 2008).

SYSTEM NAME AND NUMBER:

Public Records—FTC (FTC–I–6).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Office of the Secretary, Clerk of Court Division, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, and

Website Manager, Office of Public Affairs, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Email: SORNs@ftc.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.;* Executive Order 10450; Freedom of Information Act, 5 U.S.C. 552; 16 CFR 4.9.

PURPOSE(S) OF THE SYSTEM:

To make appropriate portions of the records in FTC matters available to the public; to enable members of the public to review and comment on or respond to such comments; to maintain records of Commission activities related to those matters.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Participants in Commission investigations, rulemaking, advisory, and law enforcement proceedings; parties requesting formal advisory opinions; consumers who have received redress or who are entitled to redress pursuant to Commission or court orders; and commenters to Commission proceedings, including general requests for comments. (Businesses, sole proprietorships, or corporations are not covered by this system.)

CATEGORIES OF RECORDS IN THE SYSTEM:

Public comments and other records that an individual may submit in an agency matter, where such record is subject to routine inspection and copying under the FTC's Rules of Practice, 16 CFR 4.9(b). These records can for example relate to general requests for information, investigations, rulemaking, advisory, and law enforcement proceedings. These records include records that either have become or are likely to become the subject of subsequent requests for substantially the same records under the Freedom of Information Act (FOIA). See 5 U.S.C. 552(a)(2)(D). This system (FTC I–6) is limited to files and records that are about an individual, and only when the file or record is pulled (''retrieved'') by the name of that individual or other identifying particular assigned to that individual (*e.g.,* number, symbol, fingerprint, etc.). Public comments received in connection with FTC rulemakings, workshops and consent agreements are also collected on behalf of the FTC and maintained by the Government-wide Federal Docket Management System (FDMS) through a website (*www.regulations.gov*). The General Services Administration (GSA) manages and operates the FDMS on behalf of the Federal Government, and has published a system of records notice to cover the FDMS, including any records collected on behalf of the FTC through that system. See GSA/OGP–1 (e-Rulemaking Program Administrative System).

RECORD SOURCE CATEGORIES:

Individual respondent(s), company records, complainants, informants, witnesses, participants, commenters, and FTC employees.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system may be:

(1) Disclosed on the FTC's public record under the FTC's Rules of Practice, including by posting copies of such records on the FTC's website, *www.ftc.gov,* or made public by other electronic or non-electronic means. See 16 CFR 4.9(b); or

(2) Disclosed publicly through the FDMS or for any other routine use set forth in the system of records notice published for that system of records, GSA/OGP–1, or any successor system notice for that system.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55541, 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The FTC maintains these records in electronic and non-electronic formats. The FTC maintains electronic records in this system using a combination of different databases and applications, rather than maintaining them in a single electronic system.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by respondent's, participant's, commenter's, or FTC staff member's name; company name; industry investigation title; FTC matter name; and FTC matter number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of under applicable schedules and procedures approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The FTC's websites are secured and monitored to protect against unauthorized deletion or alteration of records posted on such sites. Access to the official record copy of such records is restricted, where appropriate, to agency personnel or contractors whose responsibilities require access. See GSA/OGP–1 (e-Rulemaking Program Administrative System) for a description of the safeguards by the Federal Docket Management System for any public comments filed in connection with FTC matters or proceedings that are found at *www.regulations.gov.*

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

87 FR 964–974 (January 7, 2022)

73 FR 33591–33634 (June 12, 2008).

* * * * *

SYSTEM NAME AND NUMBER:

Office of Inspector General Files—FTC (FTC–I–7).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Office of Inspector General (OIG), Federal Trade Commission, 600

Pennsylvania Avenue NW, Washington, DC 20580. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022). Also see *https://www.ftc.gov/office-inspector-general/reports-correspondence.*

SYSTEM MANAGER(S):

Inspector General, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Inspector General Act, as amended, 5 U.S.C. 401 *et seq.*

PURPOSE(S) OF THE SYSTEM:

The OIG maintains this system of records to carry out its responsibilities pursuant to the Inspector General Act, as amended. The OIG is statutorily directed to receive complaints and conduct and supervise investigations, reviews and audits relating to programs and operations of the Federal Trade Commission, to promote economy, efficiency, and effectiveness in the administration of such programs and operations, and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system consist of complaints and related correspondence concerning possible violations of law, rules, regulations, mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health or safety related to the FTC; records created, received, or obtained during the course of investigating individuals and entities suspected of having committed illegal or unethical acts or misconduct and in any resulting related criminal prosecutions, civil proceedings, or administrative actions; and records created, received, or obtained during the course of conducting audits, inspections, or reviews and issuing reports, advisories or correspondence.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered consist of: (1) current and former FTC employees, applicants for employment, contractors and subcontractors associated with an activity that OIG is investigating, inspecting, reviewing, or auditing; (2) individuals who submit complaints to the OIG; (3) subjects of hotline complaints; and (4) individuals and entities performing some other role of significance to the OIG's investigative, inspecting, reviewing, or auditing efforts, such as potential witnesses or subjects who are not FTC current or former employees, contractors or subcontractors. The system also tracks information related to OIG staff and staff of other agencies involved in conducting the investigative, inspecting, reviewing or auditing activity.

CATEGORIES OF RECORDS IN THE SYSTEM

Records related to complaints to the OIG, planning and conducting investigations, reviews, inspections and audits, the results of investigations, and any civil, criminal, or administrative actions resulting from investigations and other matters. More specifically, this includes, but is not limited to, correspondence relating to investigations and other matters; internal staff memoranda; copies of subpoenas issued during investigations and other matters, affidavits, statements from witnesses, transcripts of testimony taken in investigations or other matters and accompanying exhibits; documents, records or copies obtained during investigations and other matters; interview notes, documents and records relating to investigations and other matters; opening reports, information or data relating to alleged or suspected criminal, civil or administrative violations or similar wrongdoing by subject individuals and final reports of investigation and other matters.

RECORD SOURCE CATEGORIES:

Employees or other individuals on whom the record is maintained, non-target witnesses, FTC and non-FTC records, to the extent necessary to receive, review and respond to complaints and carry out OIG investigations, reviews, inspections, and audits, as authorized by 5 U.S.C. 401 *et seq.*

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system may be:

1. Disclosed to agencies, offices, or establishments of the executive, legislative, or judicial branches of the federal or state government—

(a) Where such agency, office, or establishment has an interest in the individual for employment purposes, including a security clearance or determination as to access to classified information, and needs to evaluate the individual's qualifications, suitability, and loyalty to the United States Government, or

(b) Where such agency, office, or establishment conducts an investigation of the individual for the purposes of granting a security clearance, or for making a determination of qualifications, suitability, or loyalty to the United States Government, or access to classified information or restricted areas, or

(c) Where the records or information in those records are relevant and necessary to a decision with regard to the hiring or retention of an employee or disciplinary or other administrative action concerning an employee, or

(d) Where disclosure is requested in connection with the award of a contract or other determination relating to a government procurement, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the record is relevant and necessary to the requesting agency's decision on the matter, including, but not limited to, disclosure to any Federal agency responsible for considering suspension or debarment actions where such record would be germane to a determination of the propriety or necessity of such action, or disclosure to the United States General Accountability Office, the General Services Administration Board of Contract Appeals, or any other federal contract board of appeals in cases relating to an agency procurement.

2. Disclosed to the Office of Personnel Management, the Office of Government Ethics, the Merit Systems Protection Board, the Office of the Special Counsel, the Equal Employment Opportunity Commission, or the Federal Labor Relations Authority or its General Counsel, of records or portions thereof relevant and necessary to carrying out their authorized functions, such as, but not limited to, rendering advice requested by the OIG, investigations of alleged or prohibited personnel practices (including unfair labor or discriminatory practices), appeals before official agencies, offices, panels or boards, and authorized studies or review of civil service or merit systems or affirmative action programs.

3. Disclosed to independent auditors or other private firms with which the Office of the Inspector General has contracted to carry out an independent audit or investigation, or to analyze, collate, aggregate or otherwise refine data collected in the system of records, subject to the requirement that such contractors shall maintain Privacy Act safeguards with respect to such records.

4. Disclosed to a direct recipient of federal funds such as a contractor, where such record reflects serious inadequacies with a recipient's personnel and disclosure of the record is for purposes of permitting a recipient

to take corrective action beneficial to the Government;

5. Disclosed to any official charged with the responsibility to conduct qualitative assessment reviews of internal safeguards and management procedures employed in investigative operations. This disclosure category includes members of the Council of the Inspectors General on Integrity and Efficiency and officials and administrative staff within their investigative chain of command, as well as authorized officials of the Department of Justice and the Federal Bureau of Investigation;

6. Disclosed to members of the Council of the Inspectors General on Integrity and Efficiency for the preparation of reports to the President and Congress on the activities of the Inspectors General;

7. Disclosed to complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of the investigation or case arising from the matters of which they complained and/or which they were a victim.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems* and at 83 FR 55541, 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The FTC maintains system records in various electronic and non-electronic formats and media. The OIG Files consist of paper records maintained in file folders, cassette tapes and CD–ROMs containing audio recordings of investigative interviews, and data maintained on computer diskettes and hard drives. The folders, cassette tapes, CD–ROMs and diskettes are stored in file cabinets in the OIG. Electronic files are retained either in FTC servers or on the cloud.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The records are retrieved by the name of the subject of the investigation or by a unique control number assigned to each investigation.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with Schedule DAA–0122–2020–0001, which was approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access is restricted to agency personnel or contractors whose responsibilities require access.. Access to electronic records is controlled by ''user ID'' and password combination, and/or role-based access controls, and/or other electronic access or network controls (*e.g.,* firewalls). Paper records are maintained in lockable rooms or file cabinets, which are kept locked during non-duty hours. FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/policy-notices/privacy-policy/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(j)(2), records in this system are exempt from the provisions of 5 U.S.C. 552(a), except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10) and (11) and (i) and corresponding provisions of 16 CFR 4.13, to the extent that a record in the system of records was compiled for criminal law enforcement purposes.

Pursuant to 5 U.S.C. 552a(k)(2), the system is exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H) and (I) and (f) and the corresponding provisions of 16 CFR 4.13, to the extent the system of records consists of investigatory material compiled for law enforcement purposes, other than material within the scope of the exemption at 5 U.S.C. 552a(j)(2). See 16 CFR 4.13(m).

HISTORY:

74 FR 17863–17866 (April 17, 2009).
73 FR 33591–33634 (June 12, 2008).

* * * * *

II. Federal Trade Commission Personnel Systems of Records

* * * * *

SYSTEM NAME AND NUMBER:

Personnel Security, Identity Management, and Access Control Records System–FTC (FTC–II–11).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. System data pertaining to identity management are maintained separately off-site by an FTC contractor. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Security Officer, Administrative Services Office, Office of the Executive Director, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580 (Personnel Security) and

Chief Human Capital Officer, Human Capital Management Office, Federal Trade Commission, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580 (Physical Security).

Email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Homeland Security Presidential Directive–12 (HSPD–12).

PURPOSE(S) OF THE SYSTEM:

To conduct personnel security investigations; to make determinations required based upon the results of those investigations; and to maintain records of the investigations and determinations; to issue credentials that comply with Government-wide standards issued under HSPD–12, or to issue other non-HSPD–12 temporary identification for access to FTC facilities or resources; to maintain logs or other records of such logical and physical access by FTC staff, contractors, or other individuals; to detect, report and take appropriation action against improper

or unauthorized issuance or use of FTC credentials, and unauthorized access to or use of FTC facilities and resources.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Current and former FTC employees, contractor staff, or other individuals who have requested, been issued, and/or used FTC identification for access to FTC and/or other Federally controlled facilities.

CATEGORIES OF RECORDS IN THE SYSTEM:

Names, security investigation reports, adjudication files, card files, and position sensitivity designation files, and other data compiled, generated or used for personnel security clearance; fingerprints, photographs, signatures, and other personal data collected or used in connection with the issuance of FTC identification (credentials); time, date, location, or other data, logs, tapes, or records compiled or generated when such credentials are used to obtain physical or logical access to FTC facilities or resources.

These records are also covered by the applicable system notice published by the Defense Counterintelligence and Security Agency (DCSA) (DUSDI 02-DoD) (Personnel Vetting Records System), and any successor system notice that may be published by DCSA for this system. Any materials obtained from DCSA remain property of DCSA and are subject to DUSDI 02-DoD.

RECORD SOURCE CATEGORIES:

Individual requesting or requiring FTC identification for logical or physical access purposes, Defense Counterintelligence and Security Agency (DCSA) Security/Suitability Investigations Index files, FBI Headquarters investigative files, fingerprint index of arrest records, Defense Central Index of Investigations, previous employers, references identified by record subject individual, school registrars, and responsive law enforcement agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) Records in this system may be used to disclose to an agency in the executive, legislative, or judicial branch, in response to its request, information on the issuance of a security clearance or the conducting of a security or suitability investigation on individuals who, at the time the records are added to the system, were Commission employees.

(2) Access logs, tapes, or other system records may be reviewed or referred and disclosed to police or other law enforcement personnel for purposes of investigating possible criminal or other illegal activity of individuals who have accessed FTC facilities or resources.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper and electronic records, tapes, or other digital or non-digital media. Identity management system data are maintained in an off-site database maintained and operated by a contractor on behalf of the FTC.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Paper records indexed by individual's name. Electronic records searched and retrieved by name or other data fields or codes.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Personnel investigation reports are retained for 15 years or until an employee separates from the agency. Records of adjudicative actions are maintained for two years. Other records in this system are retained and destroyed in accordance with applicable retention and disposal schedules and guidance issued or approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to personnel security files is restricted to FTC Personnel Security staff, and such files are maintained in a FedRAMP certified electronic case management system. Any hard copy materials are maintained in a combination-locked safe and lockable metal file cabinets in locked rooms. Personnel investigation reports may be reviewed by an agency official (who has been subject to a favorable background investigation) only on a strict need-to-know basis. Identity management system (IDMS) data are collected, maintained and accessed only by authorized individuals. IDMS data are not maintained with other data on agency network servers, but are transferred by dedicated telephone data lines for off-site vendor storage, management and security. Security systems and equipment that electronically log or record usage of FTC-issued credentials to obtain access to FTC facilities or resources are secured electronically and physically (*e.g.,* recording and video monitoring equipment and servers in rooms accessible only by authorized key cards). FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(5), records in this system, to the extent such records have been compiled to determine suitability, eligibility, or qualifications for employment or other matters, as set forth in the cited Privacy Act provision, and would reveal the identity of a confidential source, are exempt from the requirements of subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of 5 U.S.C. 552a. See § 4.13(m) of the FTC Rules of Practice, 16 CFR 4.13(m).

HISTORY:

73 FR 33591–33634 (June 12, 2008).

* * * * *

IV. Correspondence Systems of Records

SYSTEM NAME AND NUMBER:

Consumer Information System–FTC (FTC–IV–1).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. This system is operated off-site by a contractor. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Assistant Director, Division of Consumer Response and Operations, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.;* section 5 of the Identity Theft and Assumption Deterrence Act of 1998 (ITADA), 18 U.S.C. 1028 note.

PURPOSE(S) OF THE SYSTEM:

To maintain records of complaints and inquiries from individual consumers; to track and respond to such communications (*e.g.,* providing information to consumers over the phone or fulfilling requests by consumers to be mailed copies of FTC publications); identify consumer problems and issues that may lead to law enforcement investigations, litigation, or other proceedings; to be used in and made part of the records of such proceedings, or to be referred to other person, entities, or authorities, where appropriate, covered by other Privacy Act system of records notices; and to provide statistical data on the number and types of complaints or other communications received by the FTC. Also, to satisfy the requirement of the ITADA that the FTC compile and refer identity theft complaints to ''appropriate entities,'' and to provide useful information that may contribute to regulation and oversight of institutions and systems that play a role in or are affected by fraudulent business practices or identity theft.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

(1) Individual consumers who submit complaints to the FTC about identity theft, or the business practices of a company or individual, as well as consumers who request information or assistance.

(2) Individuals who submit their complaints about identity theft or the business practices of a company or individual to another organization that has agreed to provide its consumer complaint information to the FTC.

(3) Individuals acting on behalf of another consumer to submit the other consumer's complaint about identity theft, or the business practices of a company or individual, or to request information or assistance on behalf of another individual.

(4) Individuals who are the subjects of complaints about identity theft or about the business practices of a company or individual.

(5) FTC or contractor staff assigned to process or respond to such communications.

(6) Other system users outside the FTC (*e.g.,* law enforcement agencies authorized to have access to the system under confidentiality agreements).

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Personally identifying information about the individual who submits a complaint or requests information or assistance, including, for example, the individual's name, address, telephone number, fax number, date of birth, Social Security or credit card numbers, email address and other personal information extracted or summarized from the individual's complaint.

(2) Personally identifying information about the individual who submits a complaint or requests information or assistance on behalf of someone else, including, for example, the submitting individual's name, address, phone or fax number and email address.

(3) The name, address, telephone number or other information about an individual who is the subject of a complaint, or is allegedly associated with the subject of a complaint. (Information in the system about companies or other non-individuals is not covered by the Privacy Act.)

(4) The name and reference number of FTC or contractor staff person who entered or updated the complaint information in the database.

(5) Name, organization, and contact data for system users outside the FTC (*e.g.,* staff of other authorized law enforcement agencies).

RECORD SOURCE CATEGORIES:

Consumers and entities who communicate with the FTC; FTC staff and contractors; other law enforcement agencies and non-FTC organizations.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) Consumer complaints can be disclosed to the subject of the complaint for purposes of attempting to resolve the complaint;

(2) Identity theft complaints also can be disclosed to the three major national credit reporting agencies and other appropriate entities to fulfill the requirements of section 5 of the ITADA; and

(3) Contact data for non-FTC users of this system (*e.g.,* staff of authorized law enforcement agencies) can be shared among such users or with others within or outside the FTC to enable them to communicate with one another.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The FTC uses several applications or components to collect and share consumer data. The FTC maintains a Consumer Response Center (CRC), which gathers, processes, and updates consumer information submitted by consumers via telephone-based services and internet-based complaint forms. Consumers access a multi-channel bilingual (English and Spanish) contact center to file complaints, report instances of identity theft, receive and print an identity theft report, and request or receive consumer education materials. Consumers may also file complaints directly from their computers and mobile devices using the online ReportFraud portal, which asks consumers to answer a series of questions organized into a few simple steps. The portal can be accessed from the URLs Reportfraud.ftc.gov and *www.ftc.gov/complaint.* Consumers with cross-border e-commerce complaints may file an online complaint at *www.econsumer.gov,* which offers cross-border consumer protection information and an additional separate online cross-border complaint form. Finally, consumers may contact the CRC through postal mail. The FTC also receives data collected by other entities. External contributors include a broad array of public and private domestic and foreign organizations.. Data from such communications are entered into a structured electronic database maintained by a contractor on the agency's behalf, and accessible by Web-based interface to FTC staff, contractors, and other authorized users (*e.g.,* federal, state, local, and international law enforcement) subject to strict access and

security controls (see ''Safeguards'' below).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved and indexed by any category of data that is submitted by consumers or otherwise compiled in association with such records (*e.g.,* name, subject of the complaint).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with Schedule DAA–0122–2021–0002, which was approved by the National Archives and Records Administration. Consumer complaint entries are generally destroyed when they are 5 years old except when they are subject to litigation holds to preserve complaints.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

The system can currently be accessed by FTC staff, contractors, and other system users, such as authorized law enforcement agency personnel. This access occurs via a Web-based interface and is authorized only on a need-to-know basis to those individuals and organizations requiring access. Contractors and other non-FTC users must sign confidentiality and nondisclosure agreements, and, in some cases, are required to undergo additional security clearance procedures. Letters or other system records in paper format are maintained in lockable rooms and cabinets. Access to the electronic database requires users to have the correct ''user ID'' and password combination, individual security token code, and internet protocol (''IP'') address for the user's law enforcement agency. The system database is maintained on secure servers, protected by firewalls, access and usage logs, and other security controls. Servers are maintained in a secure physical environment, including building locks, security guards, and cameras.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008). Individuals who call the FTC's Consumer Response Center can also use their FTC reference number to identify complaints they have previously submitted in order to update them.

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008). Individuals who call the FTC's Consumer Response Center can also use their FTC reference number to identify complaints they have previously submitted in order to update them.

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008). Individuals who call the FTC's Consumer Response Center can also use their FTC reference number to identify complaints they have previously submitted in order to update them.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(2), records in this system relating to identity theft are exempt from the requirements of subsections (c)(3), (d), (e)(1), (e)(4) (G), (H), (I), and (f) of 5 U.S.C. 552a, and the corresponding provisions of 16 CFR 4.13. See FTC Rules of Practice 4.13(m), 16 CFR 4.13(m).

HISTORY:

73 FR 33591–33634 (June 12, 2008).

* * * * *

SYSTEM NAME AND NUMBER:

National Do Not Call Registry System–FTC (FTC–IV–3).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. System database is maintained and operated off-site by a contractor. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

National Do Not Call Registry Program Manager, Division of Consumer Response and Operations, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

See Treasury/FMS.017 for the system manager and address of the *www.pay.gov* system.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.,* Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. 6101–6108; Do-Not-Call Implementation Act, Public Law No. 108–10 (2003); Do-Not-Call Improvement Act of 2007, Public Law 110–187 (2008); Do-Not-Call Registry Fee Extension Act of 2007, Public Law 110–188 (2008).

PURPOSE(S) OF THE SYSTEM:

To maintain records of the telephone numbers of individuals who do not wish to receive telemarketing calls; to disclose such records to telemarketers, sellers, and their agents in order for them to reconcile their do-not-call lists with the Registry and comply with the do-not-call provisions of the Commission's Telemarketing Sales Rule, 16 CFR part 310; to enable the Commission and other law enforcement officials to determine whether a company is complying with the Rule; to provide statistical data that may lead to or be incorporated into law enforcement investigations and litigation; or for other law enforcement, regulatory or informational purposes. Information submitted by or compiled on telemarketers, sellers, and their agents is used for purposes of fee collection, authorizing their access to the system, and related purposes and uses as described in this notice.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who notify the Commission that they do not wish to receive telemarketing calls. Individually identifiable information (*e.g.,* name, email address) that telemarketers, sellers, or their agents must submit when paying for and obtaining access to the system is covered by this system only to the extent, if any, that such information is ''about [the] individual'' within the meaning of the Privacy Act, and is not about the telemarketer, seller, or agent acting in a non-individual business capacity.

CATEGORIES OF RECORDS IN THE SYSTEM:

Telephone numbers of individuals who do not wish to receive telemarketing calls; information automatically generated by the system, including date and/or time that the telephone number was placed on or

removed from the Registry; and other information that the individual may be asked to provide voluntarily (such as email address, if the individual registers through the National Do Not Call Registry website). Telemarketers, sellers, and their agents are also required to submit information to pay for and obtain authorized access to the system, including the names of, or other identifiers that may be associated with, individuals (*e.g.,* name of contact person, name of the person to whom the credit card is issued, email address, etc.). Such information is part of this FTC system of records only to the extent, if any, that such information is maintained in the FTC's records and is ''about [the] individual'' within the meaning of the Privacy Act, and not about a telemarketer, seller, or agent acting in a non-individual business capacity.

Otherwise, user fee payment data from telemarketers, sellers, and their agents required to participate in the National Do Not Call Registry are principally collected and maintained on behalf of the Government by the *www.pay.gov* website operated by the Department of Treasury Financial Management Service (FMS). Those data are covered by the applicable system notice published by Treasury/FMS, Treasury/FMS.017 (Collections Records), and any successor system notice that may be published for that system.

RECORD SOURCE CATEGORIES:

Individuals who inform the Commission through the procedures established by the Commission that they do not wish to receive telemarketing calls. Some records may come from do-not-call lists that some states or organizations separately maintain. Record sources for this system may also include telemarketers, sellers, and agents, but only to the extent, if any, that they are ''individuals'' within the meaning of the Privacy Act.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) Telephone numbers, but not any email addresses, submitted by individuals may be made available or referred on an automatic or other basis to telemarketers, sellers, and their agents for the purpose of determining or verifying that an individual does not wish to receive telemarketing calls;

(2) Information submitted by or compiled on telemarketers, sellers, and their agents may be used and disclosed to other Federal, state, or local government authorities for payment or billing purposes, including referral to debt collection agencies or other governmental entities for collection, tax reporting, or other related purposes. Information that is submitted by or compiled on telemarketers, sellers, and their agents and that is incorporated into the *www.pay.gov* system shall also be subject to routine uses, if any, that may be separately published for that system, Treasury/FMS.017 (Collections Records), or any successor system notice for that system.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in the system are collected and maintained by an off-site FTC contractor in an electronic database with Web-based access subject to strict security controls (see ''Safeguards'' below).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by area code and phone number of individuals who have informed the Commission that they do not wish to receive telemarketing calls. May also be retrieved by other data, if any, compiled or otherwise maintained with the record. For information submitted by or compiled on telemarketers, sellers, or their agents, records may be indexed and retrieved by any category of data that is submitted by or compiled on such telemarketers, sellers, or agents.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with Schedule DAA–0122–2021–0002, which was approved by the National Archives and Records Administration. Consumer complaint entries are generally destroyed when they are 5 years old except when they are subject to litigation holds to preserve complaints. The consumer registration function allows consumers to register their telephone numbers in the DNC system and to verify whether their phone numbers are on the registry. These registration entries are deleted 20 years after request of the individual to whom the telephone number is assigned, or the phone number is disconnected and reassigned. Telemarketer registrations are deleted 20 years after the telemarketer account no longer has any active subscriptions. The retention and destruction of payment data collected from telemarketers, sellers, and their agents by Treasury's FMS is described in the system notice for the *www.pay.gov* system, Treasury/FMS.017.

The Spam Database, which was retired in 2019, provided the public with an email address to which they could forward email and text messages that they believed to be spam. This database will be deleted on October 1, 2032.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access is generally restricted to those agency personnel, contractors and other law enforcement users subject to confidentiality agreements whose responsibilities require access, or to approved telemarketers, sellers, and their agents. Electronic access is subject to login ID, password, and other electronic access and security controls (*e.g.,* firewalls). Contractors are required to sign confidentiality and nondisclosure agreements.

RECORD ACCESS PROCEDURES:

To request access to any information maintained with your registration that is not available to you through the automated dial-in system or the designated website described in the notification procedures above, you must submit your request in writing. See Appendix II (How To Make A Privacy Act Request) for details. The same access procedure applies to the extent, if any, that the Privacy Act applies to information submitted by or compiled on telemarketers, sellers, or their agents, where that information is not made available for review or amendments when the telemarketer, seller, or agent accesses the system.

CONTESTING RECORD PROCEDURES:

Where an individual believes the system has erroneously recorded or omitted information that is collected and maintained by the system, the individual will be afforded the opportunity to register, change, or delete that information after the automated system identifies and verifies the telephone number from which the individual is calling, if the individual is using the designated website, or the individual provides other identifying information, if requested by the automated system. To contest the accuracy of any other information that is not accessible to the individual through the automated dial-in system or website as described in the

''Notification procedures'' section above, the request must be submitted to the FTC in writing. See Appendix II (How To Make A Privacy Act Request) for details. The same written request requirement applies to telemarketers, sellers, or their agents (to the extent, if any, that they are ''individuals'' within the meaning of the Privacy Act) when seeking to contest the accuracy of system information maintained on them, except for system information, if any, that can be contested or corrected through the automated system.

NOTIFICATION PROCEDURES:

To obtain notification of whether the system contains a record pertaining to that individual (*i.e.,* the individual's telephone number), individuals use a dial-in system or a designated website that will enable the identification and verification of their telephone numbers. Individuals filing written requests pursuant to 16 CFR 4.13 will be acknowledged and directed to use those automated systems. To the extent, if any, that the Privacy Act applies to information submitted by or compiled on telemarketers, sellers, or their agents, the system provides notice (*i.e.,* confirms) that the system is maintaining such information when an individual accesses the system using the account number that was previously assigned to the telemarketer, seller, or agent at the time that entity originally entered information into the system to establish the relevant account.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

74 FR 17863–17866 (April 17, 2009).
73 FR 33591–33634 (June 12, 2008).

* * * * *

VII. Miscellaneous Systems of Records

* * * * *

SYSTEM NAME AND NUMBER:

Automated Library Management System–FTC (FTC–VII–1).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Head Librarian, Library, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*

PURPOSE(S) OF THE SYSTEM:

To manage the FTC Library's acquisition and collection of books, periodicals and other publications; to fulfill requests for the routing of serials among FTC employees; to electronically index or search for holdings in the FTC Library's collection.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

FTC personnel who request that copies of FTC Library periodicals or other publications in the Library's collection be routinely circulated (routed) to them within the FTC; authors of books, periodicals, or other publications indexed in the Library's collection; and other individuals that request FTC Library materials through inter-library loans.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name and office location of the FTC individual making a routing request, employee identification number, and the name and number of the periodical; names of authors or other individuals indexed or associated with books or other publications maintained in the FTC Library's collection or requested through inter-library loans.

RECORD SOURCE CATEGORIES:

Individual about whom the record is maintained; author or other publication data associated with the book, periodical or other publication; system users.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

For ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic database using a commercially available software application.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by periodical number, employee identification number, author, or other information in the system.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of in accordance with applicable schedules and procedures issued or approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access restricted to staff or contractor personnel whose responsibilities require access. Access to electronic records is controlled by ''user ID'' and password combination and/or other appropriate electronic access or network controls (*e.g.,* firewalls). (This limitation does not apply to searchable online catalog made available in the FTC Library.) FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How To Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

73 FR 33591–33634 (June 12, 2008).

* * * * *

SYSTEM NAME AND NUMBER:

Matter Record Search System (MaRS)–FTC (FTC–VII–6).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. For other locations where records may be maintained or accessed, see Appendix III (Locations of FTC Buildings and Regional Offices), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 87 FR 57698 (Sept. 21, 2022).

SYSTEM MANAGER(S):

Office of the Secretary, Records Management Division, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, email: *SORNs@ftc.gov.*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*

PURPOSE(S) OF THE SYSTEM:

To provide staff with the ability to search for and access copies of agency documents needed for legal and economic research activities of the Commission (*e.g.,* internal memoranda, economic reports, other agency work product); to provide FTC staff processing Freedom of Information Act or other disclosure requests with the ability to search for and access copies of potentially responsive documents outlining the actions and considerations of the Commission, individual Commissioners, and the staff; to provide the ability, once the automated system is fully implemented, to electronically manage the writing, editing, storage, retrieval and disposal of such documents (*e.g.,* memoranda, correspondence), and to provide for additional document management functions, if any.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have written documents contained in Commission files, and other individuals whose names or other personally identifying data are used to search and retrieve documents from the system.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name of author and documents written by that individual; names or other data about other individuals by which documents in the system are searched and retrieved; finding aids or document indexes. Records in this system may duplicate records included in other FTC systems of records. See, *e.g.,* FTC–I–1 (Nonpublic Investigational and Other Nonpublic Legal Program Records–FTC), FTC–I–6 (Public Records–FTC).

RECORD SOURCE CATEGORIES:

FTC employees and others who submit documents to the Commission.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Records in this system may be disclosed to contractors in connection with document processing, storage, disposal and similar records management and retrieval activities.

For other ways that the Privacy Act permits the FTC to use or disclose system records outside the agency, see Appendix I (Authorized Disclosures and Routine Uses Applicable to All FTC Privacy Act Systems of Records), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 83 FR 55541, 55542–55543 (Nov. 6, 2018).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Older records are stored on electronic and non-electronic formats. The system also comprises one or more structured databases using commercial software applications to search, retrieve, and manage records stored electronically.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Indexed by author of the document, or other data fields or codes.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and destroyed in accordance with schedules and procedures issued or approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access is restricted to agency personnel and contractors whose responsibilities require access. Paper or other non-digital records are stored in secure offsite storage or lockable file cabinets or offices. Access to electronic records is controlled by ''user ID'' and password combination, and/or role-based access controls, and/or other appropriate electronic access or network controls (*e.g.,* firewalls). FTC buildings are guarded and monitored by security personnel, cameras, ID checks, and other physical security measures.

RECORD ACCESS PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* and at 73 FR 33592, 33634 (June 12, 2008).

CONTESTING RECORD PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* at 73 FR 33592, 33634 (June 12, 2008).

NOTIFICATION PROCEDURES:

See § 4.13 of the FTC's Rules of Practice, 16 CFR 4.13. For additional guidance, see also Appendix II (How to Make A Privacy Act Request), available on the FTC's website at *https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems* at 73 FR 33592, 33634 (June 12, 2008).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Records contained in this system that have been placed on the FTC public record are available upon request or, where applicable, made available online. See FTC–I–6 (Public Records–FTC). However, pursuant to 5 U.S.C. 552a(k)(2), records in this system, which reflect records that are contained in other systems of records that are designated as exempt, are exempt from the requirements of subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), (I), and (f) of 5 U.S.C. 552a. See § 4.13(m) of the FTC Rules of Practice, 16 CFR 4.13(m).

HISTORY:

87 FR 964–974 (January 7, 2022)
73 FR 33591–33634 (June 12, 2008).

* * * * *

Joel Christie,

Acting Secretary.

[FR Doc. 2024–22391 Filed 9–27–24; 8:45 am]

BILLING CODE 6750–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[Docket No. CDC–2024–0072]

Meeting of the Advisory Committee on Immunization Practices

AGENCY: Centers for Disease Control and Prevention (CDC), Department of Health and Human Services (HHS).

ACTION: Notice and request for comment.

SUMMARY: In accordance with the Federal Advisory Committee Act, the Centers for Disease Control and