**SYSTEM NAME AND NUMBER**:

Computer Systems User Identification and Access Records–FTC (FTC-VII-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 80 FR 9460, 9465 (Feb. 23, 2015).

**SYSTEM MANAGER(S)**:

Core Engineering and ISSO Services Program Manager, Office of the Chief Information Officer, 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.; Federal Information Security Management Act of 2002, Pub. L. 107-347, Title III.

**PURPOSE(S) OF THE SYSTEM**:

To monitor usage of computer systems; to support server and desktop hardware and software; to ensure the availability and reliability of the agency computer facilities; to help document and/or control access to various computer systems; to audit, log, and alert responsible FTC personnel when certain personally identifying information is accessed in specified systems; to prepare budget requests for automated services; to identify the need for and to conduct

training programs, which can include the topics of information security, acceptable computer practices, and FTC information security policies and procedures; to monitor security on computer systems; to add and delete users; to investigate and make referrals for disciplinary or other action if improper or unauthorized use is suspected or detected.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM**:

Commission employees and others (e.g., contractors) with access to FTC computer systems, including various system platforms, applications, and databases (e.g., Outlook, Business Objects, Oracle, Redress, STAFFID, CIS, etc.), operated by the FTC or by a contractor for the FTC.

**CATEGORIES OF RECORDS IN THE SYSTEM**:

This Privacy Act system consists of the login and other user identification and access records that FTC computer systems routinely compile and maintain about users of those systems. These records include user data such as: user name; e-mail address; employee or other user identification number; organization code; systems or services to which the individual has access; systems and services used; amount of time spent using each system; number of usage sessions; and user profile. These system records include log-in, passphrase, and other system usage files and directories when they contain data on specific users. Many FTC computer systems collect and maintain additional information, other than system use data, about individuals inside and outside the FTC. See a complete list of FTC Privacy Act systems on the FTC's Web site, http://www.ftc.gov/foia/listofpaysystems.shtm, to learn about other categories of information collected and maintained about individuals in the FTC's computer systems.

**RECORD SOURCE CATEGORIES**:

Individual about whom record is maintained; internal and external information systems that record usage.

**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 developing, maintaining, operating or servicing FTC computerized systems.

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**:

Electronic and paper records.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS**:

Indexed by individual's name; employee identification number; and organization code, or other searchable data fields or codes.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS**:

Records are retained according to GRS 3.2, item 030, and are destroyed when business use ceases.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS**:

Access is restricted to agency personnel and contractors whose responsibilities require access. Paper records, if any, maintained in lockable rooms or file cabinets. Access to electronic

records is controlled by "user ID" and passphrase 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**:

None.

**HISTORY**:

80 FR 9460-9465 (February 23, 2015)

74 FR 17863-17866 (April 17, 2009)

73 FR 33591-33634 (June 12, 2008).