FTC-VII-3

SYSTEM NAME:

Computer Systems User Identification and Access Records–FTC.

SECURITY CLASSIFICATION:

Not applicable.

SYSTEM LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580. See Appendix III for other locations where records may be maintained or accessed.

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.

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):

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.

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.

See Appendix I for other ways that the Privacy Act allows the FTC to use or disclose system records outside the agency.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None, except as authorized under 5 U.S.C. 552a(b)(12) when trying to collect a claim of the Government. See Appendix I.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Electronic and paper records.

RETRIEVABILITY:

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

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.

RETENTION AND DISPOSAL:

See National Archives and Records Administration General Records Schedule 20.1 (Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records) and 24.6 (User Identification, Profiles, Authorizations and

Password Files). Records are deleted when no longer needed for administrative, legal, audit, or other operational purposes.

SYSTEM MANAGER(S) AND ADDRESS:

Assistant Chief Information Officer, Infrastructure Operations, Office of Information and Technology Management, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580.

Assistant Chief Information Officer, Operations Assurance, Office of Information and Technology Management, Federal Trade Commission, 600 Pennsylvania Avenue, NW., Washington, DC 20580.

NOTIFICATION PROCEDURE; RECORD ACCESS PROCEDURES; AND CONTESTING RECORD PROCEDURES:

See Appendix II.

RECORD SOURCE CATEGORIES:

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

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.