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:

89 FR 79598-79610 (September 30, 2024)

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