Federal Trade Commission
Privacy Impact Assessment

Personnel Investigative Tracking System

November 2012

1. System Overview

The Federal Trade Commission (FTC) Security Office uses the Personnel Investigative Tracking System (PITS) to maintain current, readily accessible information about the status of background investigations, security clearances, and other security-related checks that are required for FTC personnel, contractors, consultants, student interns, vendors, and others who have access to FTC facilities and networks. (The system is not used to maintain any information about members of the public.) PITS is a standalone database, accessible only to authorized Security Office personnel, that contains only the limited personal information necessary to identify each individual, together with information about that individual's current security status, such as the dates on which security checks were initiated and completed, and the determinations regarding that individual's background and security clearance, including eligibility for access to classified national security information and sensitive but unclassified information and eligibility for access to classified national security information.

PITS does not contain personnel files, the detailed information that is collected in connection with the background check and security clearance process, or the complete results of the security checks; those materials are maintained separately and securely in the access-controlled Security Office. The Personally Identifiable Information (PII) contained in PITS consists of information that is extracted from existing FTC systems and personnel forms to permit identification of the individual, and subsequent information that is provided to the Security Office in connection with background clearance, security checks, and other security-related processes. All such information is manually entered into PITS by authorized Security Office personnel.

PITS is primarily used internally by the FTC, but information from PITS may be shared, when relevant and necessary, with the Office of Personnel Management (OPM) (in connection with background checks), the Scattered Castles Secure Compartmented Information (SCI) personnel security database operated by the Director of National Intelligence (DNI) (in rare cases when an applicant may require access to classified matters),[1] and the Personal Identity Verification (PIV) Management System (in connection with the issuance of Government ID badges) for the Homeland Security Presidential Directive 12 (HSPD-12) system.[2]

The E-Government Act of 2002 and Office of Management & Budget (OMB) Memorandum 03-22 do not require a Privacy Impact Assessment (PIA) when the system does not collect information in identifiable form about members of the public. Nevertheless, the FTC has conducted this PIA to analyze and ensure that the agency has addressed the privacy impact of this system on the employees and other individuals working at the FTC whose data are maintained in the system.

---

[1] See http://www.dni.gov/files/documents/ICPG/icpg_704_5.pdf

[2] See the separate FTC PIA for its PIV card system posted at http://www.ftc.gov/ftc/privacyimpactassessment.shtm

2. Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

PITS includes the following information about FTC employees, contractors, consultants, student interns, vendors, and others who have access to FTC assets:

- Full name
- SSN
- Address
- Date of birth
- Place of birth
- Race
- Duty location
- Location
- Employee type
- Organization
- Position type
- Position sensitivity
- Access level
- Whether clearance forms have been received and date completed
- Date clearance forms validated as complete and correct.
- Whether fingerprints have been forwarded to OPM/Federal Bureau of Investigation (FBI)
- Date fingerprints results received form FBI
- Credit check completed and date completed
- Date suitability determination
- Enter-On-Duty (EOD) date
- Employment status
- Separation date
- Organization code
- Job series
- Contractor status
- Contractor company
- Contractor start date
- Contractor end date
- Company contact
- OPM investigation scope
- SCI clearance notification dates including brief and debrief dates
- Case status
- Pay plan
- Grade/Step
- Release date
- Contracting Officer’s Representative (COR)

2.2 What are the sources of the information in the system?

FTC employees, contractors, consultants, student interns, vendors, and others who require access to FTC facilities and systems. The information initially comes from personnel questionnaire forms completed by these individuals, and is manually entered into the system by Security Office personnel, who periodically update the system to reflect the status of the individual's background clearance and security checks. See Section 2.4.

2.3 Why is the information being collected, used, disseminated, or maintained?

PITS is used to track compliance with, completion of, and current status of the background investigations and security clearances that are required by Executive Order 10450 to determine an individual's eligibility and suitability for work at a federal agency.

2.4 How is the information collected?

The information that is manually entered into PITS by authorized Security Office personnel is obtained from forms completed by individuals – the SF-85 *Questionnaire for Non-Sensitive Positions* and SF-86 *Questionnaire for National Security Positions* – and/or from OPM's e-QIP system.[3]

2.5 How will the information be checked for accuracy and timeliness (currency)?

Individuals complete and submit their information directly by form SF-85 and SF-86 and/or electronically via OPM's e-QIP system, as discussed in 2.4, above. The Security Office selects certain elements of that information for manual entry into PITS and verifies, corrects, or updates that information in the course of the background checks and security clearance

2.6 Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

No.

2.7 What law or regulation permits the collection of this information?

Depending on the type of background clearance or security check required, collection of the information, including the information included in PITS, is authorized by Executive Orders 10450 (as amended), 10865, 12333, and 12356; sections 3301 and 9101 of Title 5, U.S. Code;

---

[3]OPM's e-QIP system was created as part of OMB's E-Government initiative and serves as a centralized source for information provided by prospective federal employees in anticipation of background checks and security clearances.

sections 2165 and 2201 of Title 42, U.S. Code; sections 781 to 887 of Title 50, U.S. Code; and parts 5, 731, 732, and 736 of Title 5, Code of Federal Regulations.

2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

The major privacy risks are unauthorized access to and misuse of significant amounts of personal information and sensitive information regarding security clearance status of individuals. PITS access by authorized Security Office personnel does not raise significant additional privacy risks, because these individuals typically already have access to the underlying sources of the data that are manually entered into PITS (e.g., investigatory files or application forms). In light of the sensitivity of the PITS information, however, access controls, training, and audit mechanisms have been implemented to ensure the appropriate use of that information.

Because of these risks, access to PITS and to the underlying sources of information – forms, e-QIP, and other sources – from which information is manually entered into PITS is strictly limited to authorized Security Office personnel. PITS access must be approved by either the Chief Security Officer or the Deputy Director of the Administrative Services Office, and all authorized PITS users receive FTC Computer Security training and are vetted and cleared for access to sensitive and classified information. For authorized users, access to PITS is limited to the minimum access necessary for their specific function – only a limited number of authorized users have the ability to update information – and access to and use of PITS is automatically tracked and audited by the Security Office. Likewise, PITS does not maintain more data elements about an individual than necessary for Security Office personnel to identify the individual and to track and facilitate his or her background and/or security clearance checks. See Section 2.1 above.

3. Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

PITS is used to track the status of all background checks and security clearances for FTC personnel, contractors, consultants, student interns, visitors, and others who have access to FTC facilities and networks during their FTC tenure.

3.2 Which internal entities will have access to the information?

Direct access to PITS and to the underlying information that is manually entered into PITS is limited to authorized Security Office personnel. Information about background checks and security clearances for particular individuals is shared with appropriate FTC employees and contractors on a need-to-know basis in connection with investigations and determinations regarding security eligibility and clearances, including authorized individuals from the Security Office, the Administrative Services Office, and the Office of the Executive Director. These

individuals, by law and contract, are bound by the Privacy Act and internal procedures for protecting such data.

3.3 Which external entities will have access to the information?

External entities cannot directly access PITS. Information in PITS, like the underlying information that is manually entered into PITS, is shared externally by authorized Security Office personnel only to the extent necessary to permit completion of background checks and security clearances or to facilitate national security clearance reciprocity and access to controlled facilities. For example, the status of background investigations, verification of security clearance, and eligibility information, together with relevant personal data, is shared with OPM, the SCI database, and the PIV Management System.

4. Notice and Access for Individuals

4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

Individuals seeking FTC employment and/or access to FTC facilities and networks are notified that they must provide this information to permit the completion of the background check and security clearance process. The SF-85 *Questionnaire for Non-Sensitive Positions* and SF-86 *Questionnaire for National Security Positions* forms and OPM's e-QIP system all provide notice to individuals, in accordance with the Privacy Act, 5 USC 552(a), regarding the reasons for collecting information, the consequences of failing to provide the requested information, and the uses of the information.

4.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. However, a background check and suitability determination are required for federal employment, so individuals who choose not to provide the requested information are not eligible for federal employment and also may not serve as a government contractor at a federal facility for a period of more than six months.

4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

No. Individuals may choose not to provide the requested information, as discussed in 4.2, above. However, individuals who choose to submit the requested information cannot limit its use, and all information submitted will be used in accordance with the notice discussed in 4.1, above.

4.4 What are the procedures that allow individuals to gain access to their own information?

The information is self-reported by individuals undergoing the background check and security clearance process when they submit their completed SF-85 and SF-86 forms and/or enter their information into e-QIP. Once that information has been submitted, individuals may contact the Security Office or the FTC's Privacy Act/FOIA Office to gain access to their personally identifiable information. See Rules 4.11(a) (FOIA procedures) and 4.13 (FTC Privacy Act procedures). Each individual is notified of, and has the ability to correct, address, and provide mitigating information related to any negative information that is identified in connection with the Security Office's completion of the background check and security clearance process. However, as noted above, PITS does not contain the assessments and only tracks, but does not generate any clearance analyses or determinations. PITS plays no role in determining or resolving any negative information and, as a result, there are no specific provisions for contesting PITS information. If a negative employment decision is made based on a negative finding, individuals also have appeal rights and the ability to request information regarding their case via the Freedom of Information Act (FOIA) office.

The contact information for the FTC FOIA Office is:

Federal Trade Commission
FOIA/Privacy Office
600 Pennsylvania Avenue, NW
Washington, DC 20580

4.5 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Other than the risk of unauthorized access to and misuse of individual records, described above, there are no additional privacy risks associated with providing individuals with access to their own records. To minimize the risks, individuals cannot directly access their own records in PITS but must request access through the Security Office or make a formal request through the FOIA Office. See Rules 4.11(a) (FOIA procedures) and 4.13 (FTC Privacy Act procedures).

5. Web Site Privacy Issues

5.1 Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon).

Not applicable.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

Not applicable**.**

5.3 If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.

Not applicable.

5.4 Explain how the public will be notified of the Privacy Policy.

Not applicable.

5.5 Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.

Not applicable.

5.6 If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

Not applicable.

6. Security of Information in the System

6.1 Are all IT security requirements and procedures required by Federal law being followed to ensure that information is appropriately secured?

Yes. The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure the information in PITS is appropriately secured.

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

Yes. PITS is part of the FTC's Data Center General Support System (GSS), which has received a Certification and Accreditation (C&A).

6.3 Has a risk assessment been conducted on the system?

Yes. A risk assessment was completed on the Data Center GSS as part of the C&A. A risk assessment was performed on the Personnel Investigative Tracking System during its testing process. In this process, appropriate security controls were identified and implemented to protect against risk to the data contained in the system.

6.4 Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.

No. PITS is a stand-alone system that can only be accessed by authorized Security Office personnel.

6.5 What procedures are in place to determine which users may access the system and are they documented?

Access to PITS is limited to Security Office personnel involved in the investigation and adjudication of personnel suitability and clearances. The scope of access to PITS is tailored to specific roles within the Security Office and to the information that an individual needs to access. Roles and access rights must be authorized by the Supervising Personnel Security Specialist, the Chief Security Officer, or a designated representative. The access-related procedures are documented in the FTC Master Security Plan. The Master Security Plan outlines the process and procedures for doing security related functions. The document outlines the personnel that will have access to the system.

6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

All FTC employees and contractors receive annual privacy and security training and, in addition, have undergone necessary background investigations and/or security clearances to permit them access to sensitive, privacy or classified information and secured facilities.

6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

PITS access and use is automatically tracked and audited by the Security Office, including a weekly review of security and application logs, monthly review of system usage reports, and a quarterly assessment of audit findings.

6.8 State that any questions regarding the security of the system should be directed to the FTC's Information Assurance Manager.

Any questions regarding the security of the system should be directed to the FTC's Information Assurance Manager.

7. Data Retention

7.1 For what period of time will data collected by this system be maintained?

The data in PITS relating to individuals is retained and disposed of in accordance with Item 1.5 (Security) of FTC's comprehensive records retention schedule that has been approved by the National Archives and Records Administration (NARA). The data is disposed of six years after separation of the employee or, for contractors, six years after the termination of the contract. Information on PITS access and use is disposed of when no longer needed for audit purposes.

7.2 What are the plans for destruction or disposal of the information?

All records and other information that includes inputs, outputs, system documentation, and system content will be disposed of in accordance with OMB, NARA, and National Institute of Standards and Technology (NIST) regulations and guidelines.

7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

See section 2.8 regarding privacy risks identified in the data retention and how those risks have been mitigated. The data will be disposed of in a manner that makes it impossible to recover

8. Privacy Act

8.1 Will the data in the system be retrieved by a personal identifier?

Yes.

8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

Yes. PITS includes information that is considered part of the FTC Privacy Act system called **II-11 -- Personnel Security, Identity Management, and Access Control Records System -- FTC**. A copy of the SORN may be downloaded from the FTC's SORN page: http://www.ftc.gov/foia/listofpaysystems.shtm. As explained in the SORN, 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 certain access and other requirements of the Act. See § 4.13(m) of the FTC Rules of Practice, 16 C.F.R. 4.13(m). Nonetheless, as discussed earlier, individuals may be granted access to their records for purpose of disputing adverse suitability determinations under certain circumstances.

(As noted in the SORN for this records system, the system is exempt from certain provisions of the Privacy Act to the extent that the records would reveal a confidential source.)

9. Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.

10. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Charles King
Chief Security Officer

Reviewed by:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Information Assurance Manager

_____ Date:_____
Jeff Nakrin
Director, Records and Filings Office

Approved:

_____ Date:
Jeff Huskey
Chief Information Officer