Federal Trade Commission
Privacy Impact Assessment

Personnel Investigative Tracking System (PITS)

Updated April 2019

PIA Template Version 1.5 – July 2017

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC) Personnel 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 also used to maintain information about prospective staff (i.e. members of the public) who have received a tentative offer of employment. The Physical Security Office uses PITS as part of the Personnel Identity Verification (PIV) badging process. PITS is a standalone database accessible to authorized Personnel Security and Physical Security staff (collectively, security personnel) and to a limited number of authorized staff and contractors in the Office of the Chief Information Officer. PITS 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.This information may include information on individuals' 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 Personnel Security file room. 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 Personnel Security Office in connection with background clearance, security checks, and other security-related processes. All such information is manually entered into PITS by authorized personnel security specialists.

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

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

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; 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 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check <u>all</u> that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☒ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☐ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Location, Duty location (Headquarters vs. Regions),Case Number
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☒ Social Security Number		
☐ Mother's Maiden Name		

Note: Although the PITS application contains fields to identify an individual's salary, these fields are not routinely used.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The PITS application contains four main tabs: Subject Demographics, Case Administration, Investigation Tracking, and Adjudication and Clearance. In addition to the PII listed in 2.1, these tabs contain other information relating to those four topics, such as investigation type/scope, investigation status, clearance status/level, information related to the progress of the investigation, relevant dates (such as investigation start/end dates, dates forms and documents were received/sent, and enter-on-duty date), and record verification/activity status. PITS contains information about actions taken regarding a clearance, such as whether a clearance was revoked. PITS contains open-text fields where users can take notes.

PITS also contains other information relating to PITS users/administrators. For instance, PITS audit log data includes information about which users/administrators added or deleted users or records, and when these actions took place. PITS also contains information about whether PITS users have administrator-level access.

2.3 What is the purpose for collection of the information listed above?

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. The Physical Security office uses PITS to perform background and identity verification checks for all personnel receiving a PIV card or Facility Access Card. All PII elements listed above are necessary for these purposes.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
FTC employees, contractors, consultants, student interns, vendors, and others who require access to FTC facilities and systems. Also, prospective FTC staff (i.e. members of the public).	The information initially comes from personnel questionnaire forms completed by these individuals, and is manually entered into the system by Personnel Security Specialists, who periodically update the system to reflect the status of the individual's background clearance and security checks. For example, Personnel Security Specialists update the system to reflect investigation initiation, scheduling, completion, and adjudication. The information that is manually entered into PITS by authorized Personnel Security Specialists is obtained from

	forms completed by individuals – the SF-85 *Questionnaire for Non-Sensitive Positions, the SF-85P Questionnaire for Public Trust Positions,* and SF-86 *Questionnaire for National Security Positions* – and/or from OPM's e-QIP system

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	***How and Why the Data Will Be Accessed/Shared***
FTC Personnel Security Staff	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.
FTC Physical Security Staff	The Physical Security office uses PITS to perform background and identity verification checks for all personnel receiving a PIV card or Facility Access Card.
FTC OCIO IT Staff/Contractors	FTC OCIO administrators have access to PITS for back-end maintenance purposes.
Investigative groups	On rare occasions, data from PITS could be provided to groups such as the Office of the Inspector General or the Insider Threat Working Group for authorized investigative purposes.
External entities	External entities cannot directly access PITS. Information in PITS, like the underlying information that is manually entered into PITS, is shared externally by authorized Personnel Security 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.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes. Some personnel security and physical security staff with access to PITS are contractors. Additionally, a small number of OCIO IT contractors have access to PITS for back-end maintenance purposes and can view all data in PITS. All FTC contractors are required to sign NDAs, complete security and privacy training prior to obtaining access to any FTC systems, and complete annual security and privacy training to maintain network access.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

The contractors referenced in 3.2 above are onsite contractors who are covered by the FTC's Breach Notification Response Plan.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☐ Notice is provided via (*check all that apply*):

- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): 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

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Yes, individuals have the opportunity to decline to provide information. 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.

Individuals who choose to submit the requested information cannot limit its use. However, all information submitted will be used in accordance with the notice discussed above.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

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 Personnel Security Office or the FTC's Privacy Act/FOIA Office to gain access to their personally identifiable information. See Rule 4.11(a) (FOIA procedures), 16 C.F.R. 4.11(a). Individuals must follow the FTC's Privacy Act rules and procedures, published in the Code of Federal Regulations at 16 C.F.R. 4.13, for requests for information. Privacy Act requests must be made in writing and submitted to the FTC's Office of General Counsel. See the FTC FOIA website and online FOIA request form. The Office of General Counsel may deny access to records that are legally exempt from disclosure. The mailing address of the FTC FOIA office is:

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

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

Each individual is notified of, and has the ability to correct, address, and provide mitigating information related to, any unfavorable adjudicative determination that is identified in connection with the Personnel Security Office's completion of the background check and security clearance process. Specifically, individuals who receive an unfavorable adjudicative determination are notified of the determination in writing, and the written message also contains instructions on how to respond to or challenge the determination. For example, individuals may be asked to contact the FTC Personnel Security Office, who could refer them to the Office of Personnel Management, the FTC Freedom of Information Act Office, or other groups as appropriate. If a negative employment decision is made based on a negative finding, individuals have appeal rights and the ability to request information regarding their case via the Freedom of Information Act (FOIA) office.

However, as noted above, PITS does not contain the assessments; PITS only tracks, but does not generate, any clearance analyses or determinations. PITS plays no role in determining or resolving any negative information relating to the clearance process. Nevertheless, if FTC staff or contractors are concerned that *inaccurate* (as opposed to negative) information about them is stored in PITS (for example, they are concerned that PITS lists the wrong case status for their investigation), they may contact the Personnel Security Office or make a formal request through the FOIA office.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Information entered into PITS about current or prospective employees is gleaned from forms that the individuals, themselves, fill out and submit, so the information is likely to be accurate. Information on these forms can be cross-referenced with other forms individuals submit to the Human Capital Management Office for accuracy, if needed. For further detail, see Section 2.4 above.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes.

Some administrative procedures and technical safeguards apply specifically to PITS:

> For instance, PITS accounts are created by a designated Personnel Security administrator, who verifies that the prospective account holder has a business need to access the system and creates accounts accordingly. Only employees/contractors with PITS accounts have access to PITS. Access to PITS is controlled using a username and password. Additionally, Social Security numbers (SSNs) in PITS are encrypted, although they are viewable by authorized PITS users to complete their job functions. Only administrators can edit SSN values or delete a record in PITS. For further information about PITS safeguards, see the risk analysis in 8.1 below.

Other administrative procedures and technical safeguards apply not only to PITS, but to many other applications at the FTC, as well:

> PITS is an application within the FTC network. In general, the FTC network is only accessible via multi-factor authentication using government-furnished equipment.
>
> All FTC positions are assigned a risk designation that has associated criteria for personnel screening. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews in accordance with OPM guidance. Before any new employee, contractor, or volunteer can access FTC applications, that individual must first attend new employee orientation and successfully complete the FTC's Privacy and Security Awareness training. All employees are granted basic network access to include email services, the Internet, the Intranet, network shared drives, network-based applications, and are assigned their own home directory. Categories of employees deemed to be higher risk – such as interns and International Fellows – may have restricted access to network and physical space.

Supervisors and/or Contracting Officer's Representatives (CORs) must identify and approve employee requests to access network applications and specify the appropriate user role and level of access privileges. Auditing measures and technical safeguards are in place commensurate with the Moderate-Impact Baseline of the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (SP) 800-53.

FTC staff is responsible for minimizing PII and disposing of it when the PII is no longer needed and in accordance with appropriate records disposition schedules. The FTC ensures that all staff and contractors annually electronically certify their acceptance of FTC privacy responsibilities and procedures by requiring comprehensive Information Security and Privacy Awareness training. Moreover, all staff must annually acknowledge procedures for handling PII – including minimizing PII – and attest that all PII maintained by the individual has been properly secured and accounted for as part of the FTC's annual privacy and security training.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

☒ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

The Personnel Security Office and OCIO will follow National Archives and Records Administration (NARA) GRS 5.6, item 190, when retaining and disposing of data in PITS.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

PITS uses a web application via the FTC intranet, but this web application is not available to the public.

8 Privacy Risks and Evaluation

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

Risk	***Mitigation Strategy***
Information contained in PITS may be inaccurate or incomplete.	See 4.3-4.4, 5.1 above.
Individuals who have access to PII could exceed their authority and use the data for unofficial/unauthorized purposes.	Personnel security staff with access to PITS are provided on-the-job training. The Personnel Security office also has a PITS user manual to guide the appropriate use of the system. In addition, as described in the user manual, PITS has logging capabilities that could assist in the detection of unauthorized application use. All FTC staff are trained on privacy and security responsibilities as described in 5.2 above.
Data could be retained in PITS longer than is needed, which may increase the risk of misuse or compromise	See 6.1 above.
Individuals who are not authorized to access PITS could gain access to PITS	Technical and procedural safeguards are in place to mitigate this risk: see 5.2 above.
PITS could be compromised in a cyberattack	The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements to ensure the information in PITS is appropriately secured.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

Yes. See information on technical safeguards, such as multi-factor authentication and username/password, in Section 5.2 above.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

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.)

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The Privacy Office routinely collaborates with system/application owners as part of its Privacy Continuous Monitoring Strategy to ensure that the information in PIAs, including this one, is accurate and to mitigate any privacy risks, as needed. Members of the public with questions or comments on the FTC's privacy practices may contact the Chief Privacy Officer using the contact information at ftc.gov/privacy.