

U.S. Securities and Exchange Commission

**Entellitrak Background Investigations (BI) Accelerator Case
Tracking System (BI/e-Pass)
PRIVACY IMPACT ASSESSMENT (PIA)**



March 24, 2022

Office of Support Operations

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

Section 1: System Overview

1.1 Name of Project or System

Entellitrak Background Investigations (BI) Accelerator Case Tracking System (BI/e-Pass)

1.2 Is the system internally or externally hosted?

- Internally Hosted (SEC) Office of Information Technology (OIT)
Externally Hosted
 (Contractor or other agency/organization)

1.3 Reason for completing PIA

- New project or system
 This is an existing system undergoing an update
First developed: 6/28/2011
Last updated: 7/12/2019
Description of update: The update includes the addition of Tyler Technologies Entellitrak Background Investigations Accelerator (BI/e-Pass) Edition version (current version 3.36)

1.4 Does the system or program employ any of the following technologies?

- Electronic Data Warehouse (EDW)
 Social Media
 Mobile Application (or GPS)
 Cloud Computing Services
 www.sec.gov Web Portal
 None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

BI/e-Pass is a customized implementation of Tyler Technologies' Entellitrak data management and workflow system and is internally hosted by the SEC. The system is used solely by the Office of Support Operations (OSO), Personnel Security Operations, Office of Security Services (OSS) staff. BI/e-Pass is a centralized repository to manage and adjudicate the background investigation (BI) process and maintain investigation record information for each SEC employee, contractor, and intern. Authorized SEC users access BI/e-Pass using a standard web browser.

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

Information is covered by Office of Personnel Management (OPM) System of Records Notice (SORN) Central-9 "Personnel Investigation Records," publicly available at <https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-central-9-personnel-investigations-records.pdf>

Specific authorities are EO 10450, as amended; EO 13488, as amended; and 5 CFR Part 731.

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

- No

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

- Yes
If yes, provide the purpose of collection: The SSN is collected as a requirement to investigate applicants for employment and SEC employees and contractors.
If yes, provide the legal authority: EO 10450, as amended; EO 13488, as amended; and 5 CFR Part 731 mandate suitability check of all employees. 5 CFR Part 302 applies to excepted service employment.

2.4 Do you retrieve data in the system by using a personal identifier?

- No
 Yes, a SORN is in progress
 Yes, there is an existing OPM SORN, Central-9 "Personnel Investigations Records."

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

- No
 Yes
If yes, please cite all relevant OMB collection numbers and their expiration dates.

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The privacy risk related to the purpose of collection includes personal information is collected without a clear purpose or without clear legal authority. This risk is mitigated by collecting information as authorized and in accordance with the collection purpose identified in the underlying SORNs listed in Section 2.4.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

- The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Social Security Number | <input checked="" type="checkbox"/> Alien Registration | <input type="checkbox"/> Financial Accounts |
| <input type="checkbox"/> Taxpayer ID | <input type="checkbox"/> Driver's License Number | <input type="checkbox"/> Financial Transactions |
| <input type="checkbox"/> Employee ID | <input checked="" type="checkbox"/> Passport Information | <input type="checkbox"/> Vehicle Identifiers |
| <input type="checkbox"/> File/Case ID | <input type="checkbox"/> Credit Card Number | <input type="checkbox"/> Employer ID |
| <input type="checkbox"/> Other: Click here to enter text. | | |

General Personal Data

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Marriage Records |
| <input checked="" type="checkbox"/> Maiden Name | <input checked="" type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Financial Information |
| <input checked="" type="checkbox"/> Alias | <input checked="" type="checkbox"/> Home Address | <input type="checkbox"/> Medical Information |
| <input checked="" type="checkbox"/> Gender | <input checked="" type="checkbox"/> Telephone Number | <input checked="" type="checkbox"/> Military Service |
| <input checked="" type="checkbox"/> Age | <input checked="" type="checkbox"/> Email Address | <input checked="" type="checkbox"/> Mother's Maiden Name |
| <input type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Education Records | <input type="checkbox"/> Health Plan Numbers |
| <input checked="" type="checkbox"/> Civil or Criminal History | <input checked="" type="checkbox"/> Zip Code | |
| <input checked="" type="checkbox"/> Other: Reports of Investigations; Arrest Records; Written Inquiries; Case Closing Transmittal (CCT), Certification (CERT), and the adjudication form OFI 79A | | |

Work-Related Data

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Occupation | <input checked="" type="checkbox"/> Telephone Number | <input type="checkbox"/> Salary |
| <input checked="" type="checkbox"/> Job Title | <input checked="" type="checkbox"/> Email Address | <input checked="" type="checkbox"/> Work History |

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

- | | | |
|--|---|--|
| <input checked="" type="checkbox"/> Work Address | <input type="checkbox"/> Certificate/License Number | <input type="checkbox"/> Business Associates |
| <input checked="" type="checkbox"/> PIV Card Information (UPN number only) | <input type="checkbox"/> Fax Number | |
| <input type="checkbox"/> Other: Click here to enter text. | | |

Distinguishing Features/Biometrics

- | | | |
|---|---|--|
| <input type="checkbox"/> Fingerprints | <input type="checkbox"/> Photographs | <input type="checkbox"/> Genetic Information |
| <input type="checkbox"/> Voice Recording | <input type="checkbox"/> Video Recordings | <input type="checkbox"/> Voice Signature |
| <input type="checkbox"/> Other: Click here to enter text. | | |

System Administration/Audit Data

- | | | |
|---|--|--|
| <input type="checkbox"/> User ID | <input type="checkbox"/> Date/Time of Access | <input type="checkbox"/> ID Files Accessed |
| <input type="checkbox"/> IP Address | <input type="checkbox"/> Queries Ran | <input type="checkbox"/> Contents of Files |
| <input type="checkbox"/> Other: Click here to enter text. | | |

3.2 Why is the PII listed in Question 3.1 collected, used, shared, or maintained by the system or project?

Information is collected from individuals seeking employment at the SEC, per EO 10450, as amended; EO 13488, as amended, and 5 CFR Part 731, to provide OSO/OSS personnel necessary information to make suitability determinations for hiring employees, contractors, and interns. If applicable, the information may also be used to make determinations regarding access to classified information for individuals. Collected information is maintained for historical purposes and used to make future suitability determinations as needed.

3.3 Whose information may be collected, used, shared, or maintained by the system?

- SEC Employees
Purpose: In order to facilitate suitability determinations as well as security clearance determinations for certain personnel.
- SEC Federal Contractors
Purpose: In order to facilitate suitability determinations as well as security clearance determinations for certain personnel..
- Interns
Purpose: In order to facilitate suitability determinations as well as security clearance determinations for certain personnel.
- Members of the Public
Purpose:
- Employee Family Members
Purpose:
- Former Employees
Purpose:
- Job Applicants
Purpose: In order to facilitate suitability determinations as well as security clearance determinations for certain personnel.
- Vendors
Purpose:
- Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

Only the required PII necessary to conduct a background investigation is collected as authorized by the OPM SORN identified in Section 2.2. Live data is never used for testing, training, and/or research efforts.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

- No.
- Yes.
NARA retention schedule DAA-GRS-2017-0006-0025.

3.6 What are the procedures for identification and disposition at the end of the retention period?

Personnel security records for SEC employees, contractors, and interns are maintained until they become inactive, at which time they are destroyed 5 years after employee or contractor relationship ends, in accordance with NARA retention schedule DAA-GRS-2017-0006-0025.

3.7 Will the system monitor members of the public, employees, and/or contractors?

- N/A
- Members of the Public
Purpose:
- Employees

Purpose:
- Contractors
Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The privacy risk is inadvertent or unauthorized disclosure of sensitive information. Safeguards in place to mitigate this risk include data encryption when sensitive information is in transit between organizations (i.e., OPM and SEC). Access controls are implemented so that only authorized SEC employees and contractors are granted access to the system.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

- Privacy Act Statement
Notice is provided on the Option Form (OF) 306 "Declaration for Federal Employment"
- System of Records Notice
OPM Central-9 "Personnel Investigation Records"
- Privacy Impact Assessment
Date of Last Update: 7/13/2018
- Web Privacy Policy

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

- Other notice:
When scheduling an appointment to receive an SEC Personal Identity Verification (PIV) credential in conjunction with the background investigation, applicants are provided a privacy and security notice at <https://www.fedidcard.gov/privacy-and-security-notice>
- Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

The primary privacy risk is inadequate notice to the user of the purpose of the collection that enables them to make an informed decision to provide the information requested. This risk is mitigated by providing a Privacy Act Statement at the point of information collection, OPM Central-9 "Personnel Investigation Records" SORN, and this PIA providing a description of the purpose and use of PII collected.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

Not applicable because the application does not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

5.2 Will internal organizations have access to the data?

- No
- Yes

Organizations:

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

There is minimal risk to privacy from internal sharing because information collected from individuals and suitability determination are only shared with authorized SEC Office of Human Resources (OHR) personnel.

5.4 Will external organizations have access to the data?

- No
- Yes

Organizations: OPM only as discussed below in question 5.5.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

A potential identified privacy risk is the unauthorized sharing of personal information with individuals not authorized to receive such information. This risk is minimal and mitigated because personal information stored in BI/e-Pass is shared externally with OPM only. OPM is the only external user of the data, as they are the agency responsible for investigating employees for the SEC.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

- Directly from the individual.

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

- Other source(s): OPM/DoD investigators collect information, which is made available to the SEC through the OPM-SEC interface.

6.2 What methods will be used to collect the data?

The data is collected through OPM's e-QIP System directly from potential SEC employees and contractors during the onboarding process. Authorized SEC Personnel Security staff log into eQIP as an end user and upload the eQIP form (pdf format), from an employee/contractor candidate, into the Entellitrak system.

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

PII is collected via e-QIP and optional form OF 306, "Declaration for Federal Employment", directly from the individual, minimizing the risk of error. Data is manually reviewed by OSS Personnel Security staff during and after the information is entered in e-QIP by the individual. When information collected is questionable, Personnel Security staff contact the individual to confirm information collected.

6.4 Does the project or system process, or access, PII in any other SEC system?

- No
 Yes.
System(s):

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is the risk of inaccurate data being entered. This risk is minimized by directly having the individual enter the information directly into eQIP.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

Individuals have the right to decline to provide data to OPM and the SEC with the understanding that doing so may result in the denial of employment at the SEC. Once data is provided, individuals do not have the right to consent to particular uses of data.

7.2 What procedures are in place to allow individuals to access their information?

Individuals seeking access to their information contained in the system may submit a request in writing to FOI/PA, Office of Personnel Management, National Background Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618 or emailing FOIPRequests@nbib.gov. Individuals may submit their request using Form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, mailing address and email address (to receive materials electronically), any available information about the records being requested, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

7.3 Can individuals amend information about themselves in the system? If so, how?

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

Individuals seeking to amend information about themselves contained in the system, or seeking to contest its content, may submit a request in writing FOI/PA, Office of Personnel Management, National Background Investigations Bureau, P.O. Box 618, 1137 Branchton Road, Boyers, PA, 16018-0618, in writing. Individuals may submit their request by using form INV100 Freedom of Information, Privacy Act Record Request Form or by sending the following information: full name, date of birth, place of birth, SSN, precise identification of the records to be amended, a statement about and evidence supporting the reasons for the request (including all available information substantiating the request); mailing address and email address to which correspondence should be sent, a signed and notarized statement or an unsworn statement declaring that the information submitted is true, and copies of two identity documents.

7.4 Discuss the privacy risks related to individual participation and redress. How were these risks mitigated?

There is a risk that individuals may not have the opportunity to correct, access, or amend inaccurate information maintained by other agencies and submitted to e-QIP. This risk is partially mitigated by publishing clear instructions on the National Background Investigation Bureau (NBIB) website, in the OPM/Central 9 SORN, and in this PIA to inform individuals about how to access and request amendment to their records, as expressly permitted by the Privacy Act.

Section 8: Security

8.1 Can the system be accessed outside of a connected SEC network?

No

Yes

If yes, is secured authentication required?

No

Yes

Not Applicable

Is the session encrypted?

No

Yes

Not Applicable

8.2 Does the project or system involve an online collection of personal data?

No

Yes

Public

URL:

8.3 Does the site have a posted privacy notice?

No

Yes

N/A

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC staff and contractors receive initial and annual privacy awareness training, which outlines roles and responsibilities for proper handling and protection of PII. SEC Rules of the Road ensure that employees and contractors are aware of their security-related responsibilities and how to fulfill them.

9.2 Does the system generate reports that contain information on individuals?

No

Yes

Privacy Impact Assessment

Entellitrak Background Investigation Accelerator Case Tracking System

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

- No
- Yes
- This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

- No
- Yes

9.5 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Although access to this system is limited only to authorized SEC staff, the expected residual risk related to access, given the sensitivity of the PII in the system, can include the inadvertent handling or misuse of data. To mitigate this risk, user accounts for employees are synched with SEC's Active Directory and system privileges are granted based on defined roles.