Date of Approval: **December 02, 2022**

PIA ID Number: **7434**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Automated Background Investigation System, ABIS

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Automated Background Investigations System (ABIS), PIAMS # 4877

What is the approval date of the most recent PCLIA?

3/16/2020

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

IRS, Human Capital Office, HCO HR Operations, Talent Acquisition

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e., system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

The Automated Background Investigations System (ABIS) is used to initiate, adjudicate, manage, analyze, and report background investigations and national security clearances for IRS employee applicants, IRS Contractors, Treasury Chief Counsel Employees and contractors, Executive Resource investigations, and other possible other agencies conducted under reimbursable agreements as deemed by management. The investigation itself is completed by Defense Counterintelligence and Security Agency (DCSA). After completion DCSA send the investigation back to IRS via eDelivery Connect Direct to ABIS. The investigation is then adjudicated by Personnel Security Specialists using ABIS. The ABIS system also stores tracking information for post appointment arrest and Treasury Inspector General for Tax Administration cases forwarded to adjudicating authorities. The ABIS program also stores tracking information for post appointment arrest, continuous evaluation, and Treasury Inspector General for Tax Administration cases forwarded to the responsible adjudicating authorities. The ABIS program is used by IRS Personal Security (PS), IRS employment offices, IRS Contract office representatives, IRS Contractors and other IRS employees that have a need for access. All access requests are processed through the Business Entitlement Access Request System (BEARS) and in accordance with Federal Information Security Management Act (FISMA) requirements. The responsibility for adjudication of background investigations for IRS applicants/employees who occupy a national security clearance position falls under the jurisdiction of the Associate Director, Personnel Security (PS) Additional information can be referenced directly from IRM 10.23 - Personnel Security: IRM 10.23.1 - National Security Positions and Access to Classified Information: IRM 10.23.2 - Contractor Investigations: IRM 10.23.3 - Personnel Security/Suitability for Employment and Personnel Security Operations.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e., last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Security Background Investigations

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

Use of SSN is needed to ensure positive identification of the subject of the investigation or security clearance.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

The SSN is only displayed in full as needed to determine and verify identity. ABIS case numbers are used internally after a case is established. Truncation to the last four digits is also used as appropriate. There is no current plan to fully eliminate use of SSN in investigative records. Use of SSN is still needed to ensure positive identification. The Office of Personnel Management (OPM) sets these standards for all government agencies.

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
Mailing Address
Phone Numbers
E-mail Address
Date of Birth
Place of Birth
Mother's Maiden Name
Criminal History
Certificate or License Numbers
Passport Number
Alien Number
Biometric Identifiers
Employment Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

The following are stored in ABIS for current and recently-employed employees/contractors with retained cases: SSN; Date and place of birth; Employee status, position title, business unit, series and grade; Credit report results; OPM investigative report results, including past employment, education, arrest and conviction records; Military data (DD-214); Tax compliance information - whether or not the person has paid any taxes due or is non-compliant; Citizenship data; Spouse and immediate family names, birth dates, citizenship and address for high risk level investigations; Current/past suitability and national security clearance granted/revoked data.

Cite the authority for collecting SBU/PII (including SSN if relevant).

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The U.S. Government needs the requested information to determine suitability for employment. The government conducts background investigations to establish that applicants/incumbents either employed, or working under contract, are suitable for the job and/or eligible for a public trust or sensitive positions, including those requiring national security clearances. The information requested is used primarily as the basis for the investigation. The investigative process cannot be completed without the information, and the subject cannot be hired, retained (if requested for a periodic reinvestigation) or granted a needed security clearance if the information is not provided.

How is the SBU/PII verified for accuracy, timeliness, and completion?

SBU/PII is entered into the system by IRS Employment Office staff and Contract Vendors who work directly with the subjects of the investigations. Information is gathered from the subject on forms such as the Declaration of Federal Employment OF306 or directly from Employment HR systems.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.016 Security Clearance Files

IRS 34.021 Personnel Security Investigations

IRS 34.022 Automated Background Investigations System (ABIS)

IRS 34.037 Audit Trail and Security Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: ALERTS (Automated Labor & Employee Relations Tracking System)
Current PCLIA: Yes
Approval Date: 2/20/2020
SA&A: Yes
ATO/IATO Date: 1/7/2020

System Name: Treasury Integrated Management Information System (TIMIS)
Current PCLIA: No
SA&A: No

System Name: PDS (Personal Identity Verification Data Synchronization)
Current PCLIA: Yes
Approval Date: 11/21/2022
SA&A: Yes
ATO/IATO Date: 11/21/2022

Does the system receive SBU/PII from other federal agency or agencies?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: eDelivery
Transmission Method: IBM Connect Direct
ISA/MOU: Yes

Name: ODNI CES
Transmission Method: IBM Connect Direct
ISA/MOU: No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

Yes

Please identify the form number and name:

Form Number: Optional Form 306
Form Name: Declaration for Federal Employment

Form Number: Standard Form 85, 85P, 86
Form Name: Investigation Request Forms

Form Number: Resume
Form Name: Resume

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: TCA (Tax Check Application)
Current PCLIA: No
SA&A: No

System Name: PDS (Personal Identity Verification Data Synchronization)
Current PCLIA: No
SA&A: No

System Name: ALERTS (Automated Labor & Employee Relations Tracking System)
Current PCLIA: Yes
Approval Date: 2/20/2020
SA&A: Yes
ATO/IATO Date: 1/7/2020

Identify the authority.

IRM 10.23.1, IRM 10.23.2, IRM 10.23.3

For what purpose?

Personal Identity Verification Data Synchronization (PDS) - ABIS shares PII background investigation adjudication data on a real-time daily basis with PDS. PDS also shares this data with both internal IRS systems and Treasury and uses it to establish qualifications for issuing or revoking PIV credentials for IRS employees. ABIS is a client of the PDS web service. The data is fully contained within the IRS network and is transferred between ABIS/PDS via

HTTPS/SSL protocols using user IDs, password, and a certificate. Career Connector Companion (CComp) (module of People Trak (PTrak) - Files containing adjudication data for approved new hires is sent nightly via Enterprise File Transfer Utility (EFTU) to a shared folder and retrieved by the IRS Career Connector application. Data is used by Employment Office staff to begin and track the Smart ID issuance process. Automated Labor and Employee Relations Tracking System (ALERTS) - BI Case Numbers and Adjudication Results are shared with the ALERTS system via a web service. ALERTS then shares any related misconduct data with ABIS

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: eDelivery
Transmission Method: IMB Connect Direct
ISA/MOU: Yes

Identify the authority.

IRM 10.23.1, IRM 10.23.2, IRM 10.23.3

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

IRS 34.016, IRS 34.021, IRS 34.022

For what purpose?

ABIS provides national security clearance status information to the Office of Personnel Management (OPM) in the form on an output file referred to as the "CVS file". CVS receives data via a manual upload to a secure portal (HTTPS) from the ABIS production server conducted by an IRS Personnel Security Adjudicator. The file is refreshed between the 8th and the 14th of each month. e-Delivery is the electronic delivery of the closed case information from OPM. Data is sent nightly via Connect: Direct with Secure Plus.

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

When the subject of the investigation goes to complete their Electronic Questionnaire for Investigations Processing(e-Qip) for their investigation they received this message before they can start: "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details." Additional due Process is always provided pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

When the subject of the investigation goes to complete their "e-Qip" for their investigation they receive this message before they can start: "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details." Additional due Process is always provided pursuant to 5 USC.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

If the subject chooses not to provide information to start the investigation process, any data ABIS has is deleted. Additional due Process is always provided pursuant to 5 USC.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Write

Contractor Developers: Administrator

How is access to SBU/PII determined and by whom?

Access to ABIS is granted only after the user goes through the Business Entitlement Access Request System (BEARS) authorization process. As part of this process, a description of the user's need to access ABIS is submitted, and access is granted according to the lowest user level that will satisfy this need. The BEARS request requires approval from the user's manager before submission. The access provided by BEARS also allows for restrictions placed on the user's activities within the ABIS screens. This forces a limitation on potential access entries beyond the scope of the user's assigned duties. Within the ABIS application, role-based access controls have been implemented. Although one user can occupy multiple roles within the software application, a user cannot be assigned as his/her own manager or work leader.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

ABIS data disposition instructions are published in Document 12990 under Records Control Schedule (RCS) 12 for Personnel Security Records, Item 2. Data retention generally depends upon the type of investigation in a case file. National Agency Check and Inquiry results provided by Defense Counterintelligence and Security Agency (DCSA) are destroyed 90 days after processing a case to a conclusion. Personnel security case files data (Item 2(a)) is approved for destruction 16 years after date of report, final legal action, or final administrative action, whichever is appropriate. Any investigative reports/related documents from investigating sources OTHER than DCSA are destroyed according to the investigating agency instructions. These are very rare and are done case-by-case. ABIS data is not retained by any contractors.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

3/22/2022

Describe the system's audit trail.

All FISMA controls, including PII safeguarding, are evaluated annually through the Annual Security Controls Assessment. The evaluation ensures all technical, operational and management controls are in place. Available in TFIMS database.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

The software is Commercial Off the Shelf (COTS) and is not tested in IRS.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: More than 100,000

Contractors: More than 10,000

Members of the Public: Not Applicable

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax, or Privacy Act consent?

No