

Date of Approval: November 08, 2023

PIA ID Number: 8309

SYSTEM DESCRIPTION

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

Automated Background Investigation System (ABIS) M, WebABIS

Is this a new system?

Yes

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

Internal Management Governance Board (IMGB) and Infrastructure Executive Steering Committee (IESC)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

WebABIS is a modernized solution to accelerate employee and contractor prescreening and eligibility/suitability determinations through workflow automation and technology modernization. ABIS Modernization will enable Human Capital Office (HCO) to increase determination velocity by 40% and reduce determination cycle time by 20% over the first year.

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

Interfaces with external entities that require the SSN

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

Required for processing background investigations.

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

None

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

Standard Employee Identifier (SEID)
Criminal History
Biometric Identifiers
Employment Information

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

No

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

No

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

PII for personnel administration is 5 USC

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.

WebABIS is used for processing background investigations on applicants, contractors, and existing federal employees. The system only captures the minimum amount of PII data that is required to process these background investigations. SSN is a required field when processing background investigations.

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

The PII (SSN) is provided directly by the subject of the investigation and validated for the number of characters, and they must all be numeric.

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.

Treasury/IRS 34.016 Security Clearance Files

Treasury/IRS 34.021 Personnel Security Investigations

Treasury/IRS 34.022 Automated Background Investigations System (ABIS)

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For 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: Position Designation Survey (PDS)

Current PCLIA: No

SA&A: No

System Name: ALERTS

Current PCLIA: Yes

Approval Date: 1/7/2022

SA&A: Yes

ATO/IATO Date: 2/23/2023

System Name: Corporate Authoritative Directory Service (CADS)
Current PCLIA: Yes
Approval Date: 9/18/2020
SA&A: Yes
ATO/IATO Date: 1/3/2020

System Name: Tax Check Application (TCA)
Current PCLIA: Yes
Approval Date: 4/1/2021
SA&A: Yes
ATO/IATO Date: 2/8/2023

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: OPM - USA Staffing
Transmission Method: Webservice
ISA/MOU: Yes

Name: DCSA E-Delivery
Transmission Method: Flat files
ISA/MOU: Yes

Name: Department of Labor/TIMIS
Transmission Method: Flat files
ISA/MOU: Yes

Name: DCSA Adjudication/Clearance holder information
Transmission Method: Flat files
ISA/MOU: Yes

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: The Declaration for Federal Employment

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: HRConnect

Current PCLIA: No

SA&A: No

System Name: PDS

Current PCLIA: No

SA&A: No

System Name: ALERTS

Current PCLIA: Yes

Approval Date: 1/7/2022

SA&A: Yes

ATO/IATO Date: 2/23/2023

System Name: TCA

Current PCLIA: Yes

Approval Date: 4/1/2021

SA&A: Yes

ATO/IATO Date: 2/8/2023

Identify the authority.

IRM 10.23.3

For what purpose?

*Eligibility checks required for employment (Tax check, and prior employment history check).
Sending status to HRConnect/PDS.*

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: DCSA

Transmission Method: Flat files

ISA/MOU: *Yes*

Identify the authority.

5CFR 731

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

Treasury/IRS 34.016 - Security Clearance Files, Treasury/IRS 34.021 - Personnel Security Investigations, Treasury/IRS 34.022 – Automated Background Investigations System (ABIS)

For what purpose?

Requirements of Personnel Security Investigations

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

3/29/2017

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

High

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

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?

It is a requirement of employment/included in the contract for contractors.

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

No

Why not?

Mandatory requirement for employment.

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

The applicants can request information access through FOIA. Applicants/contractors are given "due process" by responding to letters of interrogatory/proposal to deny where they can provide mitigating information.

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: Read Write

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

Access is determined by "Position" and the "Need to Know" as defined by the Manager.

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. or GRS 5.6, item 170, 171 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 ECM-R

Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)?

In-process

When is the anticipated date of the SA&A or ECM-R completion?

10/24/2024

Describe the system's audit trail.

Records the ip address, the origination user-id, event-timestamp, event-type, whether it is a SA action, success status, Database record access, and any pertinent additional information.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

N/A for COTS and Managed Services.

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: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

Employees at banks that process IRS Tax returns under 10,000.

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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

Continuous vetting/monitoring during a person's tenure at the agency (arrests, high value financial transactions - \$10,000 or higher, social media exchanges, etc.). This information is sent to WebABIS for review and determinations.

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