Date of Approval: 05/16/2025
Questionnaire Number: 2279

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Integrated Automation Technologies

Acronym:

IAT

Business Unit

Taxpayer Services

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Integrated Automation Technologies (IAT) is a collection of workstation-installed productivity tools used for account research and processing functions in the Integrated Data Retrieval System (IDRS.) IAT tools interface with IDRS through the InfoConnect terminal software to provide a more modern Graphical User Interface (GUI) to research, analyze, and input changes to command codes in IDRS. These tools assist employees with translating IDRS information to plain language, decision-making, following IRM technical and procedural guidance, and reducing case time and common errors. The tools are accessed and updated through the IAT software application installed on workstations of users in need of IAT tools. The IAT system is owned and operated by the IRS. It is comprised of several application and database servers, and two disaster recovery servers. These servers and system components provide IAT staff with web applications, services,

and data for developing, managing, and delivering IAT tools to customers. IAT servers store small amounts of employee PII (SEIDs, IAT employee names & emails) for reference, statistical, and operational purposes; they use standard logging and auditing which may also include PII. IAT tools receive SBU/PII from IRS files and databases, including: IDRS, Corporate Authoritative Directory Service (CADS), Withholding Compliance System (WHCS), and Examination Returns Control System (ERCS.) They disseminate SBU/PII to other IRS systems, including: IDRS, WHCS, and ERCS. The IAT software gathers tool usage statistics and exception information for troubleshooting errors during tool runtime, and sends the information to IAT services for storing, processing, and reporting. No taxpayer data is stored on IAT servers.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

IAT tools access taxpayer data through the InfoConnect terminal software, process the data, display the data, make decisions, and input actions on taxpayer accounts. All actions are based on the user's profile and access level for the systems being accessed; tools cannot perform actions beyond those the user could complete manually. Any information collected through processing of taxpayer calls or case inventory is not retained by IAT tools beyond the lifetime of that application instance. Several tools maintain data on the user's workstation in an encrypted SBU Data folder for the purpose of completing actions on numerous taxpayer accounts (batch runs), or providing automation in completing forms related to daily case processing duties. This data comes from other IRS systems, typically through previously existing reports, and not the taxpayer directly.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Centralized Authorization File (CAF)
Document Locator Number (DLN)
Email Address
Employer Identification Number
Federal Tax Information (FTI)
Financial Account Number
Internet Protocol Address (IP Address)
Name

Other
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers

Please explain the other type(s) of PII that this project uses.
Date of Birth, Place of Birth

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?
No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?
Application

3 What Tier designation has been applied to your system? (Number)
4

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
Yes

4.11 What is the previous PCLIA number?
7212

4.12 What is the previous PCLIA title (system name)?
Integrated Automation Technologies (IAT)

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)
Expiring PCLIA

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Enterprise Computing Center Change Control Board (ECC CCB)

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

210662

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?

Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

IAT tools obtain data from other IRS systems and do not own any of the data; any corrections or due process is handled by the systems that maintain and own the data. For employee data, users provide data voluntarily except for general statistics, which can be viewed and corrections requested from the IAT organization if necessary.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

Access to the system is limited to IRS Employees. Users and Managers have Read and Write access. System Administrators have Administrator access. Developers have Read-Only access.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

Any information collected by IAT tools through the processing of taxpayer calls or case inventory is not retained beyond the lifetime of the application instance and is passed into the system which users would have previously input the data manually. The information retained by a limited number of IAT tools (such as that in users' encrypted SBU Data folders) is data from other IRS systems, typically from previously existing reports, not from the taxpayer directly. Any employee information collected by IAT web applications or systems is covered by the site privacy statement. Statistical records regarding tool usage are collected under the Privacy Act Section 3(a)(6) and there is no mechanism for consent. Individual-level records are used within IAT for monitoring appropriate usage during the development lifecycle. Organizational-level records (down to team-level only) are available to IRS employees for statistical reporting purposes of tool usage within their organization or the service.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

More than 100,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

Not Applicable

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

Not Applicable

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

The IAT system utilizes the standard IRS on-line access application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access to their local management for approval. Users are not permitted access without a signed form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access. Users are assigned to specific modules of the application and specific roles within the modules and accounts follow the principle of least privilege which provide them the least amount of access to PII/SBU data that is required to perform their business function after receiving appropriate approval.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

Each piece of client-side software (tools) and server application is tested through the Enterprise Life Cycle (ELC) process detailed in the W&I Tools Development & Maintenance Guide, and all privacy concerns are identified and addressed during the design and development phase. All attempts are made to minimize the data collected during the design phase. Each application is tested during development, pre-production, and final integration testing to ensure that privacy and security controls are in place and operating appropriately. Privacy Awareness and Training is completed each year by employees through their mandatory briefings.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

Standard Enterprise-compliant auditing is performed at the operating system, database management system, and web server levels. These standards are defined and managed by Information Technologies and handled at the General Support System (GSS) level, with elements such as, but not limited to: Internet Protocol address, username, and requested query being logged.

27 Does this system use or plan to use SBU data in a non-production environment?
Yes

27.1 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request (F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.
No

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
Corporate Authoritative Directory Service (CADS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Secure Lightweight Directory Access Protocol (SLDAP)

Interface Type
IRS Systems, file, or database
Agency Name
Examination Returns Control System (ERCS)
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Transmission Control Protocol - Internet Protocol (TCPIP)

Interface Type
IRS Systems, file, or database
Agency Name
Integrated Data Retrieval System (IDRS)
Incoming/Outgoing
Both
Transfer Method
Other

Other Transfer Method
Transmission Control Protocol - Internet Protocol (TCPIP)

Interface Type
IRS Systems, file, or database
Agency Name
Withholding Compliance System (WHCS)
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Transmission Control Protocol - Internet Protocol (TCPIP)

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 36.003 - General Personnel and Payroll Records
Describe the IRS use and relevance of this SORN.
The IAT system interacts with CADS to utilize SEIDs, employee names, employee TIMIS data, and employee emails

SORN Number & Name
IRS 24.030 - Customer Account Data Engine Individual Master File
Describe the IRS use and relevance of this SORN.
IAT tools interact with IDRS to automate research and case work, which includes Individual Master File (IMF) records

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
The IAT system maintains audit trails and security records as is required by all systems

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
IAT tools interact with IDRS to automate research and case work, which includes Business Master File (BMF) records

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
Transitory and Intermediary Records
What is the GRS/RCS Item Number?
020
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
Intermediary Records. Records that exist for the sole purpose of creating a subsequent record and are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision making.
What is the disposition schedule?
Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
Information Systems Security Records
What is the GRS/RCS Item Number?
030
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
System access records. Records created as part of the user identification and authorization process to gain access to systems. Records used to monitor inappropriate systems access by users, including user profiles, log-in files, password files, audit trail files and extracts, system usage files, or cost-back files used to assess charges for system use. Systems not requiring special accountability for access. User identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.
What is the disposition schedule?
Temporary. Destroy when business use ceases.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Information Systems Security Records

What is the GRS/RCS Item Number?

031

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

System access records. Records created as part of the user identification and authorization process to gain access to systems. Records used to monitor inappropriate systems access by users, including user profiles, log-in files, password files, audit trail files and extracts, system usage files, or cost-back files used to assess charges for system use Systems requiring special accountability for access. User identification records associated with systems which are highly sensitive and potentially vulnerable.

What is the disposition schedule?

Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.