

Date of Approval: 04/05/2025
Questionnaire Number: 1842

Basic Information/Executive Summary

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

Authorization Framework On-Premise

Acronym:

AZF On-Prem

Business Unit

Information Technology

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.

Authorization Framework (AZF) is a common platform that ensures a consistent approach for access control decisions by providing centralized Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) authorizations for IRS applications across the Enterprise. Utilizing a system-oriented architecture (SOA), AZF provides a platform that integrates with existing authentication and authorization infrastructure and applications. This reduces dependency on individual commercial off the shelf (COTS) products and allows for standards-based implementations, providing a consistent approach for increased security and reduced integration time with each application.

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).

AZF has two services - Authorization and Attribute. Authorization Service - AZF receives sensitive data in body of authorization service request. Depending on the client application, AZF will connect to other Policy Information Points to request more sensitive data. Authorization service will then use this data to make an authorization decision of Permit or Deny. AZF returns the decision to the requesting application and sends a log to ESAT Splunk. Sensitive data in ESAT Splunk audit logs are destroyed after 18 months per IRM requirement. Attribute Service - AZF receives sensitive data in body of attribute service request. AZF will manipulate Attribute database depending on request body with sensitive information and will return to requesting client application success or failure message. Data is stored in AZF Attribute DB until client application destroys it based on its own attribute service requests. AZF also sends a log to ESAT Splunk. Sensitive data in ESAT Splunk audit logs are destroyed after 18 months per IRM.

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

Address

Email Address

Employer Identification Number

Federal Tax Information (FTI)

Individual Taxpayer Identification Number (ITIN)

Name

Social Security Number (including masked or last four digits)

Universal Unique Identifier (UUID)

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.2 What is the IRA Initiative Number?

1.2, 4.3, and 4.4.

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

System

1.35 Is there a data dictionary for this system?

No

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

AZF provides two services to clients - Authorization Decision Service (ADS) and Attribute Management Service (AMS). In ADS and AMS, the exact PII and FTI varies by AZF client. In that service, clients (1) send a request to AZF, (2) AZF connects with various PIP (Policy Information Point) data sources to collect more information, (3) AZF uses all the info from request and PIPs to make an authorization decision, (4) AZF returns that decision to client that sent request and logs the event in the audit and application log for the authorization decision. AMS is an optional service clients can use to store required by AZF ADS service to provide authorization decisions. Clients (1) send a request to AMS that includes attributes in database that need to be added, updated, or removed. (2) AZF processes the request once received and records the result of the action in system and audit log.

1.4 Is this a new system?

No

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes

1.6 What is the PCLIA number?

7648

1.7 What are the changes and why?

Revised requirements after onboarding new clients.

1.8 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.

211215

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?
Execution

2.1 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? Contact Disclosure to determine if an accounting is required. Enter "Yes" or "No". If Exempt, type "Exempt".

No

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

Authentication, Authorizations & Access- Executive Governance Board (A3 EGB)

3.1 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?

No

3.2 What is the methodology used and what database is training your AI?

AZF does not have or use AI.

3.3 Does this system use cloud computing?

No

3.31 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

AZF On-prem does not use CSPs.

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

AZF does not have direct users and provides backend A2A services.

Authorization Service - Attributes provided and retrieved by this service are read only and AZF does not manipulate individual's data that passes through the system in the request or PIP sources. Attribute Service - The individual's ability to access or correct their information in it is managed by each client application itself, AZF just stores the information client applications pass in their requests.

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owned and Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

No

4.3 What PII/SBU data does the subcontractor have access to?

None

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

No contractor has access to PII data.

4.51 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".

AZF only supports A2A with external RUP users, not IRS internal EUP users.

4.52 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".

No records are attributable to contracts.

4.53 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".

More than 1,000,000

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

AZF Application Team does not have access to any client PROD SBU or PII. TIGTA/ESAT has access to this info within Splunk audit logs. Authorization Service: AZF provides Authorization decisions based on individual client requirements, including what SBU/PII is accessed and by whom. Generally, specific PIPs containing attributes which may be SBU or PII are required to make the authorization decisions. Attribute Service: AZF client applications which are onboarded to this service may access their own data only. Details around where the information clients submit to our service is accessed or by whom is determined by the client application.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

There are no privacy risk, civil liberties or security risk identified.

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

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

No

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

eServices request to AZF

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Automated Lien System (ALS) request to AZF

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

AZF to ESAT Audit Records

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

Clean Energy (CE) request to AZF

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Business Taxpayer Account (BTA) request to AZF

Incoming/Outgoing

Incoming (Receiving)

Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database

Agency Name
AZF request to Enterprise Data Platform (EDP) sent to Business Master File (BMF)

Incoming/Outgoing
Both

Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database

Agency Name
AZF sends request to ALS DB

Incoming/Outgoing
Incoming (Receiving)

Transfer Method
Secured channel via HTTPS

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.

By electronic filing provider name or Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or other similar number assigned by the IRS)

SORN Number & Name

Treasury .015 - General Information Technology Access Account Records
Describe the IRS use and relevance of this SORN.

Records may be retrieved by an identification number assigned by computer, by facility, by business affiliation, email address, or by the name of the individual, or other employee data fields previously identified in this System of Records Notice.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

By name, Social Security Number (SSN), or the standard employee identification number (SEID) of employee, contractor, or other individual who has been granted access to IRS information, or to IRS equipment and resources, and by incident number. Also, by name, SSN or Taxpayer Identification Number (TIN) of entities whose records were accessed.

Records Retention

What is the Record Schedule System?

Non-Record