Date of Approval: 03/01/2024 Questionnaire Number: 1037

# **Basic Information/Executive Summary**

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

Common Business Services

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.

Common Business Services (CBS) is an Integrated Middleware, an Enterprise Services platform to access legacy data from mainframe systems and payment information from Bureau of Fiscal Services (BFS). The CBS System provides interfaces to multiple IRS backend systems using ECLAS and to external partner BFS via mutual Transport Layer Security (mTLS) Internal Protocol version 6(IPv6) Secure tunnel connectivity. Enterprise entity web services are designed to reduce the cost of development and maintenance of Information Technology (IT) systems. Customers that utilize CBS services, range from internal facing applications such as Account Management Services (AMS) to external facing applications like Online Accounts (OLA). Application hosted web services provide information to that taxpayer's entity data, calculate the taxpayer balance due, retrieve the available tax returns on file, tax return financial details, account summary, update taxpayer data in Integrated Data Retrieval Service (IDRS) like generate notices/create installment agreement, retrieve payments and create payment requests. Our purpose is to help bridge the gap from the backend systems

the modernized world, centralize enterprise business rules and serves as a gateway to process payments connecting to external partners like BFS. The interface for the CBS is an application-to-application interface and all the clients who access are within the IRS network.

## **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).

The CBS Common Services which include the Data Services (DS), and Fiscal Service Interface Gateway (FSIG) programs require the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. CBS is a middleware and does not store data.

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** 

Financial Account Number

Internet Protocol Address (IP Address)

Name

Social Security Number (including masked or last four digits)

## **Product Information (Questions)**

- 1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)? No
- 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?

Yes

1.36 Explain in detail how PII and SBU data flow into, through and out of this system. Common Business Services (CBS) is an Integrated Middleware that consist of two components Data Services (DS) and Fiscal Services Interface Gateway (FSIG). The FSIG establishes connections to the Bureau of Fiscal Services (BFS) over a virtual private network (VPN) using a secure encrypted connection. The purpose of these web services is to provide data, allowing taxpayers to view their payment history, schedule a payment, or set up/edit a payment plan. The services hosted by FSIG are SearchA Payment, MakeAPayment, CancelAPayment and ValidateBankAccount. The FSIG clients are Individual Online Account (IOLA), Business Online Account (BOLA) and Tax Professional Account (TaxPro). The DS Application retrieves taxpayer data, applies business rules on the data retrieved from legacy back-end systems (IDRS/CFOL). Services hosted by DS are Get Individual Balance Due, Get Taxpayer Primary Name, Get Individual Tax Return Modules Get Individual Return Transaction Get Raw String, Global Eligibility (IA Service), InstallmentAgreement (IA) Origination and revise Installment Agreement. Clients are IOLA, TaxPro.

#### 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? 7004
- 1.8 If the system is on the As-Built-Architecture, what is the ABA ID of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID for each application covered separated by a comma.

Yes, and the ABA # is 211262.

- 1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)? Execution
- 1.95 If this system has a parent system, what is the PCLIA Number of the parent system? Not Applicable
- 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.

Compliance Domain Governance Board (CDGB)

3.3 Does this system use cloud computing?

No, application is within the IRS data centers.

3.4 Is there a breach/incident plan on file?

CBS is a Tier 4 application and IRP is not required for this app. However, the application is hosted on GSS-42 servers so this would inherit to GSS-42.

3.5 Does the data physically reside in systems located in the United States and its territories and is all access and support of this system performed from within the United States and its territories?

Yes, the servers are located in XXXXXXX, XX and XXXXXXXXXX, XX data centers.

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

  No, this is a middleware application and does not have direct users / web interface.
- 3.61 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

There are no users. This is a Middleware application. DIRA is not required for Tier 4 application.

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

SiteMinder agents are used to establish trust between systems with security tokens. SiteMinder is a third-party application that stores credentials and resources that are to be protected. Each application must get a token from the SiteMinder host and embed that token in their request to access the system. The receiving application then sends that SiteMinder token to the SiteMinder host to validate the token is valid and the account and server that generated the token can access the resource.

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

IRS Owned

- 4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.
  - System Administrators Contractor System Administrators / Yes

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".

Not Applicable

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".

Not Applicable

- 4.53 How many records in the system are attributable to members of the public? ". Not Applicable
- 4.54 If records are attributable to a category not mentioned above in 4.51 through 4.53, please identify the category and the number of corresponding records to the nearest 10,000. If none, enter "Not Applicable".

Not Applicable

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

Contractor personnel may be employed by Operational groups for support of this AD developed system. Access to SBU data is controlled by the consumer application (IOLA, BOLA, TaxPro, and DMIAPP) and SAAS audit logs.

- 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?

  None
- 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, there is no RAFT open for this application.

- 5.2 Does this system use or plan to use SBU data in a non-production environment?
- 5.3 Please upload the approved SBU Data Use Questionnaire or Request. If the request has been recertified, please upload the approved recertification form. Select Yes to indicate that you will upload the SBU Data Use form.

Yes, we will upload the form once it's complete.

### **Interfaces**

Interface Type
IRS Systems, file, or database
Agency Name

IOLA, BOLA, TaxPro, DMIAPP, RCCMS

Incoming/Outgoing

Both

Agency Agreement

No

Transfer Method

Secured channel via HTTPS

### **Interface Type**

Other Federal Agencies

Agency Name

Bureau of Fiscal Services

Incoming/Outgoing

Both

Agency Agreement

Yes

Agreement Name

January 2023 - Interconnection Security Agreement (ISA) And Memorandum of Agreement (MOA)

Transfer Method

Secured channel via HTTPS

### **Interface Type**

IRS Systems, file, or database

Agency Name

IDRS, CFOL

Incoming/Outgoing

Both

Agency Agreement

No

Transfer Method

Secured channel via HTTPS

# **Systems of Records Notices (SORNs)**

#### **SORN Number & Name**

IRS 26.019 - Taxpayer Delinquent Account Files

Describe the IRS use and relevance of this SORN.

Provide ability for Taxpayer to view Tax Account Information on IRS.gov (IOLA, TaxPro)

#### **SORN Number & Name**

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Provide audit trails to security by logging all request for taxpayer data from IOLA, BOLA and TaxPro.

#### **SORN Number & Name**

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

Provide ability for Taxpayer to view Tax Account Information on IRS.gov (IOLA, TaxPro)

### **Records Retention**

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

General Technology Management Records

What is the GRS/RCS Item Number?

GRS 3.1 item 020

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item. CBS audit and user logs are scheduled under GENERAL RECORDS SCHEDULE (GRS) 3.1 for General Technology Management Records, Item 020. IRS System Technology audit logs are maintained per IRM 5.1.25.6 in the Security Audit and Analysis System (SAAS). Audit Logs will be erased or purged from the SAAS at the conclusion of their retention period(s) as required under IRM 1.15.6. The method used for sanitization will follow NIST SP 800-88 guidelines.

What is the disposition schedule?

retention period(s) as required under IRM 1.15.6. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. IRS Audit logs are kept for 7 years.

### **Data Locations**

What type of site is this? System

What is the name of the System?
Common Business Services (CBS)
What is the sensitivity of the System?
Federal Tax Information (FTI)