Date of Approval: **August 23, 2019**

PIA ID Number: **4295**

SYSTEM DESCRIPTION

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

Common Business Services and Fiscal Services Interface Gateway, CBS/FSIG

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?

Common Business Services Release 1, CBS 1816

What is the approval date of the most recent PCLIA?

8/9/2016

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

Adding the Fiscal Service Interface Gateway (FSIG) component which will allow applications to request taxpayer payment history from the Bureau of Fiscal Services (BFS)

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

Technical Integration Organization (TIO)

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

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.

Common Business Services (CBS) connects the On-Line Account Minimum Viable Product (OLA MVP) to IRS back end databases to retrieve taxpayer information in the form of the taxpayer's name. It then gathers what the taxpayer may owe to the IRS and calculates balances due based on accrued penalties and interest. This data is returned to the OLA MVP application so that the taxpayer may see this information. The Online Account application itself, and not the enterprise e-Authentication application, will focus on the role and privileges of the taxpayer only. This is a web-based application, accessed through irs.gov, using the Integrated Enterprise Portal (IEP). The addition of the Fiscal Service Interface Gateway (FSIG) component serves as the middleware component that connects the OnLine Account application to the Bureau of Fiscal Services (BFS). The system will be able to retrieve the payments made by a taxpayer, allow taxpayer to make a payment, and allow taxpayers to create and delete scheduled payments. The IRS is not collecting any new taxpayer information, only providing a new online channel for taxpayers to interact with the IRS.

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:

Interfaces with external entities that require the SSN

When there is no reasonable alternative means for meeting business requirements

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

In order to retrieve taxpayer information from either the back-end data stores or from the Bureau of Fiscal Services (BFS), the SSN is the only unique item that can be used to accurately retrieve this information.

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

The CBS Common Services and FSIG programs require the use of SSN's 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.

Other Taxpayer Identification Number

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

Financial Account Numbers

Tax Account 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 (SBU List)

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

Protected Information - Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

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.

FSIG will calculate penalties and interest for the taxpayer, show them any balance due and a list of payments they made as well as take or schedule a payment.

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

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 services establish the connections to the IRS Databases using a protocol called the CLAS (Consolidated Legacy Access Service) for processing information using standard multi-functional commands that access specific data within the IRS. The purpose of these interfaces called web services is to provide data needed to display the individual filers' balances that they owe to the IRS and also display the taxpayers' authoritative name on record, housed in IRS databases. 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.

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

The common business services is the middle layer between the User Interface provided by the Online Account project and the IRS databases that store IRS taxpayer data. It is incumbent on the consumer of the Common Business Services, in this case OLA MVP, to ensure that the user has been authenticated and authorized prior to submitting the request of taxpayer information on the behalf of the taxpayer and relies on existing controls within the IRS legacy databases to ensure that the data is accurate and timely. The FSIG is the middle layer between the Online Account project and the Bureau of Fiscal Services (BFS) which has the taxpayer payment information stored. It is incumbent on the consumer of the FSIG, in this case OLA MVP, to ensure that the user has been authenticated and authorized prior to submitting the request of taxpayer information on the behalf of the taxpayer and relies on existing controls within BFS to ensure that the data is accurate and timely.

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 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 26.019 Taxpayer Delinquent Accounts Files

IRS 34.037 Audit Trail and Security Records System

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: Online Account

Current PCLIA: Yes

Approval Date: 9/20/2018

SA&A: Yes

ATO/IATO Date: 1/17/2018

System Name: IDRS (Integrated Data Retrieval System)

Current PCLIA: Yes

Approval Date: 9/25/2018

SA&A: Yes

ATO/IATO Date: 6/13/2018

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: Bureau Of Fiscal Services

Transmission Method: HTTPS

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)?

No

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: Online Accounts MVP

Current PCLIA: Yes

Approval Date: 12/19/2016

SA&A: Yes

ATO/IATO Date: 12/15/2016

System Name: Security Audit and Analysis System (SAAS) Audit logs

Current PCLIA: Yes

Approval Date: 4/9/2018

SA&A: Yes

ATO/IATO Date: 6/12/2017

Identify the authority

Internal Revenue Code (IRC) Sections 6001, 6011, 6012e(a) - process taxpayer information. IRC Section 6109 - collecting SSN information.

For what purpose?

The purpose of the CBS services is to provide relevant taxpayer entity information from the data stores to the authorized requestor. The Security Audit and Analysis System (SAAS) audit logs are used to audit who requested what information and what data was sent back with that request.

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: Bureau of Fiscal Services

Transmission Method: HTTPS

ISA/MOU Yes

Identify the authority

The authority for this agreement is based on the following policy, standards and guidance: - Federal Information Security Modernization Act (FISMA) of 2014, 44 USC § 3551 et seq., as part of the E-Government Act of 2002 (as amended); - Office of Management and Budget (OMB) Circular A-130, Appendix I, Managing Information as a Strategic Resource; - National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology systems; - United States Department of the Treasury TD P 85-01, Treasury Information Technology Security Program, Unclassified Non-National Security Systems. IRC §6103(h)(1) authorizes disclosures to BFS to carry out IRS tax administration programs.

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

The FSIG system will allow IRS applications to access the information stored in the Bureau of Fiscal Services (BFS) system. The system will request payment history for a given taxpayer, allow taxpayers to schedule payments, make payments, and delete scheduled payments.

For what purpose?

The purpose is to allow taxpayers to have greater control of their payments and account history through the online tool.

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?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Explain why not required.

All authentication should be handled by the application that uses CBS/FSIG. For example, OLA/WebApps uses eAuthentication from E-Services to ensure the identity of their users.

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?

IRS.gov has several methods of informing the taxpayer about these issues. The website has a Privacy Policy which states "Using these services is voluntary and may require that you provide additional personal information to us. Providing the requested information implies your consent for us to use this data in order to respond to your specific request." Prior to using the Online Account application, Online Account has the required notice that this is a US Government system for authorized use only.

"Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties, including all penalties applicable to willful unauthorized access (UNAX) or inspection of taxpayer records (under 18 U.S.C. 1030 and 26 U.S.C. 7213A and 26 U.S.C. 7431)." Common Business Services strictly supplies taxpayer information to Online Account. The application informs the taxpayer of use of the System of Records 24.030 Individual Master File. The taxpayer is also provided a link to all IRS Privacy Impact Assessments.

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

No

Why not?

Individuals are given the privacy notices and can decide not to use the services provided.

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

There is no due process, CBS is middleware and only supplies applications (OLA) the available data. The applications choose what to display and would be responsible for any due process. OLA would be responsible for incorrect information given to the taxpayer. CBS does use SiteMinder agents 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.

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

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor System Administrators: Administrator

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 OLA MVP and SAAS audit logs.

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.

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.

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?

8/15/2016

Describe the system's audit trail.

An Audit Plan will be created for this system by the project team with the support of Enterprise System Acceptance Testing/Security Audit and Analysis System (ESAT/SAAS). It will record all actions of the taxpayer/user in near-realtime and transmit to SAAS/ESAR logs for Cybersecurity Operations review. The Audit trail is documented in the Technical Review Document for CBS Release 1, examples of some of the fields are: timestamp, application name, user ID, request type, balance due, taxpayer identification number, tax period, and return type.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

The scope of the test plan is to provide a common understanding of how CBS is approaching the distinct test types. The test types being conducted are Code and Unit Test, Integration Test, Independent System Acceptance Test (ISAT), and Regression Test. - Code and Unit Test: The first level of software testing typically performed immediately after the code is developed to test each individual component of the application. Code and Unit testing consists of physical testing of the code module or object that is performed by the developer or programmer allowing them to detect errors and remove them from software. - Integration Testing- The purpose of Integration Testing is to accept, integrate, and test software components until the entire system is operational and all agreed upon customer requirements

have been validated. During the integration test phases, the change applied to component and functionality related to the component will be tested. Integration testing focuses on testing all functionality including the integration points between the various applications. This will validate that all interfaces between systems, subsystems and external systems function as defined and can support the required functionality and performance. Independent Systems Acceptability Test (ISAT) - ISAT is required if a System Acceptability Test is not performed by Enterprise Systems Testing (EST). When performing an ISAT the activities described in IRM 2.127.2 must be followed. An ISAT assesses the quality of the application software by testing with controlled data to determine conformance of the system to customer requirements and to aid the customer and developer in determining the systems' production readiness. Regression Testing- Regression testing verifies that the system produces the expected results after changes/corrections have been applied and that code modifications have not inadvertently introduced bugs into the system or changed existing functionality. It is performed after making a functional improvement or repair to a program to ensure the changes have not caused problems in other aspects of the program. Regression testing demonstrates system integrity after changes are made to software functions. Negative or Backwards Compatibility testing will be included in both the integration and regression test phase. - 508 Compliance Testing - CBS does not have a user interface. Test documentation includes the artifacts and work products that provide evidence of successful verification of requirements. Documentation is developed to define requirements, design the change, and verify the solution through test execution. The documentation listed below will be developed in support of the test types planned. - Test scripts are saved under the CBS DocIT folder.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Testing between OLA MVP and CBS R1 using the SiteMinder enterprise agent has been conducted in all environments to ensure that security controls are in place for authorization and access controls are being adhered to. Testing with security audit logging and file transfer was also completed.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

10/24/2016 12:00:00 AM

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

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?

Yes

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.

Not Applicable

Explain the Exemption and/or Disclosure's response.

The system provides taxpayer PII to BFS under IRC 6103(h1). IRC 6103 (h)1 disclosures are exempt from the accounting requirement.