Date of Approval: September 21, 2018 PIA ID Number: **3598**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Online Account, OLA

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

Online Account, OLA, PCLIA #2002

Enter the approval **date** of the most recent PCLIA. 12/19/2016

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of Personally Identifiable Information (PII)(PII is any information that is linked or linkable).
No	Conversions
No	Anonymous to Non-Anonymous
Yes	Significant System Management Changes
No	Significant Merging with Another System
Yes	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection
No	Expiring PCLIA

Were there other system changes not listed above? No

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

Web Applications(WebApps) Governance Board and Strategic Development Executive Steering Committee. This artifact update is for the Integrated Readiness Review.

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

A.1 General Business Purpose

5. 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.
Online Account (OLA) is a Web-based application, using the Integrated Enterprise Portal (IEP), that allows individual taxpayers access to their tax information and be able to take actions on their tax accounts using a single sign-on capability. It also provides the framework for additional online capabilities to expand the taxpayer online experience. OLA implements a single sign-on with a login and password leveraging the eAuthentication system and provides a landing page that includes the following capabilities: a) See balance due, b) See payment status / history, c) Make a payment, d) Get tax records, and e) Apply and Modify installment agreement/payment plan, The IRS benefits from OLA by providing taxpayers increased availability to self-service applications, which decreases taxpayer's reliance on more expensive phone, correspondence and walk-in channels. The IRS is not collecting any new taxpayer information, only providing a new online channel for taxpayers to interact with the IRS. The OLA application itself, and not the enterprise e-Authentication application, focuses on the role and privileges of the taxpayer only. OLA uses the Web Apps Platform environments, which is the single conduit provider of common services, utilities, and components, which allows all the projects to utilize and leverage these services, supporting reusability across the enterprise. All activities and data accessed as a result of that activity may be stored for usage statistics and analytics on the Web Apps Platform.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6.a. If **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

If **yes**, check all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
Yes	Interfaces with external entities that require the SSN
No	Legal/statutory basis (e.g. where collection is expressly required by statute)
No	When there is no reasonable alternative means for meeting business requirements
Yes	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

WebApps Platform system requires 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.

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

There are no current plans to eliminate the use of SSNs. All taxpayer interactions with this system will take place through secure means and require identification through the IRS' secure access eAuthentication systems. The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If **yes**, specify the information.

Selected	PII Element
Yes	Name
No	Mailing address
Yes	Phone Numbers
No	E-mail Address
Yes	Date of Birth
No	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
Yes	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
Yes	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? No

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

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

1. OLA establishes a single online account enabling taxpayers to view, update, and retrieve their tax information. The SSN is used as an access key to retrieve and update information in other IRS systems (e.g., transcript and payment information). OLA leverages the Web Apps Platform services for auditing, analytics, and other non-functional system reporting needs. Web Apps Platform services include: 2. Usage statistics- Web and business analytics are critical components for Web Apps and target platform. Employing analytics allows the IRS the ability to improve the website's usability as well as make business decisions that improves business processes and user experiences. In addition, analytics benefits business units with recommendations and promotions, user trends analysis, fraud management, and business intelligence. SSNs are required to uniquely

identify individuals impacted by or associated with website activity. 3. Online Audit Trail- Online activity is recorded to be used in the event of criminal online activity (e.g., return fraud) for court cases. Universal User Identifiers (UUIDs) do not cover all cases: spouses, dependents, and clients of tax professionals that do not have UUIDs or other suitable identifiers. For these cases, there is no other alternative identifier, so SSNs must be used to cross correlate any fraudulent activity. Each application transaction is recorded as an audit event, extracted, and sent to Security Auditing and Analysis System (SAAS) to prove audit trail for Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigation (CI), and Cybersecurity. 4. Cybersecurity- Online activity is tracked for use in identifying and mitigating cybersecurity threats. Web Apps Platform collects web service requests and responses and copied to the Cybersecurity Data Warehouse (CSDW) that stores historical audit data and provides an offline analytic resource for Cybersecurity. 5. Diagnostics- The Custom Diagnostics solution allows internal IRS users the ability to view health of the Web Application Servers and the actual applications running on them, including user access patterns and errors, typically during production support. Custom Diagnostics could include any functionality where log data is monitored and cleansed for viewing by any internal IRS user.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

The data that OLA receives is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA.

C. 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.

9. 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

If **yes**, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
IRS 22.062	Electronic Filing Records
IRS 22.061	Information Return Master File
IRS 26.019	Taxpayer Delinquent Accounts Files
IRS 26.020	Taxpayer Delinquency Investigation Files
IRS 34.037	Audit Trail and Security Records System
IRS 37.006	Correspondence, Miscellaneous Records and Information Management Records
IRS 37.111	Preparer Tax Identification Number Records

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
eAuthentication (eAuth)	Yes	07/10/2018	Yes	10/24/2017
Common Business Services Release 1 (CBS)	Yes	08/09/2016	No	
Web Applications Platform Environments	Yes	08/07/2018	No	

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from **Taxpayer** forms? No

11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
eAuthentication (eAuth)	Yes	07/10/2018	Yes	10/24/2017
Security Audit Analysis System (SAAS)	Yes	04/13/2018	Yes	06/12/2017
Common Business Services Release 1 (CBS)	Yes	08/09/2016	No	
Cybersecurity Data Warehouse (CSDW)	Yes	11/03/2017	No	
Web Applications Platform Environments	Yes	08/07/2018	No	

Identify the authority. IRC Sections 6001, 6011, 6012e(a) - process taxpayer information. IRC Section 6109 – collecting SSN information.

For what purpose? OLA gives taxpayers access to abstracted taxpayer information residing on IRS Core systems (e.g., CBS). Online activity is recorded to be used in the event of criminal online activity. Each application transaction is recorded as an audit event, extracted, and sent to SAAS to prove audit trail for TIGTA, CI, and Cybersecurity.

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? Yes

16.a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16.a.1. If **yes**, when was the **e-RA** conducted? 08/05/2015

If **yes**, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

If **Level 2**, Confidence based on:

Knowledge Based Authentication (Out of Wallet)

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
The irs.gov has several methods of informing the taxpayer about these issues. The irs.gov 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 U.S. Government system for authorized use only. That notice is copied below: WARNING! By accessing and using this government computer system, you are consenting to system monitoring for law enforcement and other purposes. Unauthorized use of, or access to, this computer system may subject you to criminal prosecution and penalties. The taxpayer is also provided a link to all IRS Privacy Impact Assessments.

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

18.a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
The taxpayer's use of the web application is voluntary. The e-Authentication application, which is the required entry point to taxpayer applications, will require the taxpayer to click on the "Consent" button provided on the website before being allowed to proceed.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The taxpayer has due process by writing, calling, faxing or visiting the IRS. They are also provided due process rights on the tax forms.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	Yes	Read-Only	Moderate
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	No		

21.a. How is access to SBU/PII determined and by whom? Access to the data by taxpayers is determined by the taxpayer entering valid shared secrets for the purpose of authentication Once taxpayer enters shared secrets and their data matches up with the Integrated Data Retrieval System (IDRS) information to ensure that the information is correct, they are eligible to use the system. All contractors and employees must go through the Public Trust Clearance process before access is considered. Once cleared, access to WebApps Platform is obtained through the On-Line 5081 (OL5081) process. All access must be approved by the user's manager who reviews the OL5081 at the time of submission and on an annual timeframe. The system administrators/approvers will also verify group membership to ensure only the appropriate rights are granted based upon need-to-know. For non-production supporting environments users must complete the necessary Sensitive But Unclassified (live) data training, request access through the OL5081, and in some cases as outlined by the requirements set forth within the Internal Revenue Manual submit an elevated access letter that is approved by the Associate Chief Information Officer prior to granting access. The non-production environment will also routinely review access lists and verify accounts, removing

ones that are no longer necessary. Every individual is reminded of their Unauthorized Access (UNAX) requirements where they are restricted to see certain taxpayer data and, in many instances, a third-party tool is implemented to restrict access to that data.

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22.a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

OLA is non-recordkeeping and does not require a NARA-approved records control schedule to affect data disposition. Web Apps Platform is only used to onboard new software initiatives and provide the tools necessary to manage applications and services used directly by taxpayers. The IRS eAuthentication platform leveraged by Web Apps Platform was approved by NARA under Standard Form 115 (Job No. N1-58-12-6, approved 11/14/2012), updating RCS 17 by adding item 31. Online Account uses GRS references for Inputs, Outputs, and System Documentation. Listed below are the GRS references: Inputs are covered in GRS 4.3, item 020 for electronic inputs. Outputs are covered in GRS 4.3, item 031 for data files, and GRS 4.3, item 030 for ad hoc output reports. System Documentation is covered in GRS 3.1, item 051. System Access Records for Audit, Usage, and Extracts are covered under GRS 3.2, item 030.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? Yes

23.a. If **yes**, what date was it completed? 06/13/2018

23.1. Describe in detail the system's audit trail. An Audit Plan has been created for this system by the project team with the support of Enterprise Security Audit Trail (ESAT)/SAAS. The system collects legal events for TIGTA, CI, and the CSDW to establish chain of custody for each transaction within all applications to be used as evidence and prove audit trails. It records all actions of the taxpayer/user in near-real-time and transmits to ESAT/SAAS logs for Cybersecurity review.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a. If **yes**, was the test plan completed? No

If **no**, when is the test plan scheduled for completion? 10/07/2018

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? The system will go through a continuous Testing Strategy Implementation Plan due to its ongoing development. It will be assessed against the selected privacy requirements. To accomplish

this, the project not only addresses the overarching Privacy Requirements but will break down the requirements to decomposed requirements that are reviewed, implemented, tested, and documented to ensure appropriate action was taken to address them. All of this is being coordinated by the Requirement Engineering Program Office and Cybersecurity and tracked in the Rational Requirements Tool and developer security (SA-11) testing. Please note that authentication is delegated to the eAuthentication system. The project uses the eAuthentication project services to authenticate taxpayer access to the applications. In authenticating, the user will log in through the Browser and Presentation Application. The eAuthentication process will access the External Identity Store through the External Policy Server for permission enforcement. Please refer to the eAuthentication PCLIA for applicable information.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	More than 1,000,000
26.d. Other:	No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? Yes

If **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. By using taxpayer-supplied PII and IP Addresses, the IRS will have the capability to identify, locate, and monitor taxpayers. The primary purpose of doing this is to correlate website usage with other IRS processes. For example, tracking notice response rates.

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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

End of Report