Date of Approval: April 13,2018 PIA ID Number: **3253**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Security Audit & Analysis System, SAAS

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Security Audit & Analysis System, SAAS, 1045, Complete

Next, enter the **date** of the most recent PIA. 7/1/2015

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

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
Yes	Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) 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
Yes	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.

The purpose of the SAAS system is to collect security audit information. SAAS assists Cybersecurity, Business Units, and Treasury Inspector General for Tax Administration (TIGTA) to detect unauthorized intrusions and privileged access abuse. Security audit information is defined a: a chronological record of user activities that is sufficient to enable the reconstruction, review, and examination of those activities; a set of records that collectively provide evidence to support enforcement actions; a set of auditable events that include all related user actions that lead up to a particular event. The audit trail record must convey these actions (i.e. user interface activities) in the record in a useful manner such that the auditable event and related actions can be reconstructed and presented in the context in which it happened.

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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes	On Primary	Yes	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

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

The use of SSN's is authorized per Internal Revenue Code Section 6109 and there is no reasonable alternative for meeting the business requirements of this system.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
Yes	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. 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
No	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.
No	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
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

.

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

6e. 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

Yes SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

Yes PII for personnel administration is 5 USC

Yes PII about individuals for Bank Secrecy Act compliance 31 USC

Yes Information by CI for certain money laundering cases may be 18 USC

6f. 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.

The purpose of the SAAS system is to collect security audit information. SAAS assists Cybersecurity, Business Units, and Treasury Inspector General for Tax Administration (TIGTA) to detect unauthorized intrusions and privileged access abuse. Security audit information is defined as: a chronological record of user activities that is sufficient to enable the reconstruction, review, and examination of those activities; a set of records that collectively provide evidence to support enforcement actions; a set of auditable events that include all related user actions that lead up to a particular event. The audit trail record must convey these actions (i.e. user interface activities) in the record in a useful manner such that the auditable event and related actions can be reconstructed and presented in the context in which it happened.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

SAAS is an application that receives audit trails from other applications. The applications are responsible for ensuring SBU/PII is verified for accuracy, timeliness, and completeness.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

SORNS Number	SORNS Name
Treasury/IRS 34.037	Audit Trail and Security Records System
Treasury/IRS 36.003	General Personnel and Payroll Records

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

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

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

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

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Automated Collection System (ACS)	Yes	12/18/2015	Yes	01/12/2018
Automated Enrollment (AE)	Yes	02/23/2016	Yes	12/21/2017
Automated Freedom of Information Act (AFOIA)	Yes	03/18/2016	Yes	01/18/2018
Big Data Analytics (BDA)	Yes	11/03/2017	Yes	12/15/2016
Business Masterfile Case Creation Non-Filer Identification Process (BMF_CCNIP)	Yes	05/29/2015	Yes	08/24/2017
Branded Prescription Drugs (BPD)	Yes	08/17/2015	Yes	11/02/2017
Counsel Automated Systems Environment Management Information System (CASEMIS)	Yes	03/13/2015	Yes	05/10/2017
Compliance Data Environment (CDE)	Yes	03/23/2016	Yes	05/10/2017
Correspondence Examination Automation Support (CEAS)	Yes	11/06/2015	Yes	12/18/2017
Electronic Authentication (EAUTH)	Yes	09/30/2015	Yes	02/10/2017
Electronic Fraud Detection System (EFDS)	Yes	12/17/2017	Yes	04/03/2017
Electronic Federal Payment Posting System (EFPPS)	Yes	05/22/2015	Yes	01/18/2018
Embedded Quality Review System – Campus (EQRSC)	Yes	12/08/2016	Yes	03/30/2017
Embedded Quality Review System – Field (EQRSF)	Yes	03/16/2016	Yes	03/28/2017
Examination Returns Control System (ERCS)	Yes	02/07/2017	Yes	03/13/2017

External Services Authorization Management (ESAM)	Yes	11/03/2015	Yes	03/22/2017
Enterprise web-based suite of Services (eServices)	Yes	11/03/2015	Yes	03/22/2017
International Compliance Management Model FATCA International Returns (ICMM FIR)	Yes	01/30/2018	Yes	07/18/2017
Integrated Financial System (IFS)	Yes	04/27/2017	Yes	10/13/2017
Issue Management System (IMS)	Yes	08/24/2016	Yes	05/07/2017
Identity Protection Personal Identification Number (IPPIN)	Yes	03/30/2016	Yes	07/14/2015
Internet Refund-Fact of Filing (IRFOF)	Yes	03/30/2016	Yes	07/14/2015
Taxpayer Identification Number - Real Time System (ITIN RTS)	Yes	12/17/2015	Yes	01/04/2018
Modernized E File (MEF)	Yes	02/23/2016	Yes	12/21/2017
Modernized Internet Employer Identification Number (MODIEIN)	Yes	03/30/2016	Yes	07/14/2015
Order a Transcript (OAT)	Yes	03/30/2016	Yes	07/14/2015
Online Payment Agreement (OPA)	Yes	03/30/2016	Yes	07/14/2015
Reporting Compliance Case Management System (RCCMS)	Yes	10/18/2017	Yes	10/27/2017
Voice Balance Due (VBD)	Yes	03/30/2016	Yes	07/14/2015
Lead and Case Analytics Project Charter (LCA)	Yes	06/30/2018	Yes	02/14/2018
Return Integrity and Compliance Services (RICS)	Yes	03/31/2017	Yes	09/11/2017
Corporate Authoritative Directory Service (CADS)	Yes	02/06/2017	No	09/11/2017
Information Returns Master File Processing (IRMF)	Yes	03/09/2017	Yes	10/22/2015
Automated Lien System – ENTITY Case Management (ALS ENTITY)	Yes	11/16/2016	Yes	10/10/2017
Automated Manual Assessments (AMA)	Yes	06/05/2015	Yes	01/01/2018
Account Management System (AMS)	Yes	09/26/2017	Yes	04/03/2017
Integrated Data Retrieval System (IDRS)	Yes	08/28/2017	Yes	01/17/2018
Foreign Account Tax Compliance Act (FATCA)	Yes	07/18/2017	Yes	01/05/2016
Federal Student Aid IRS Datashare (FSAD)	Yes	03/30/2016	Yes	07/14/2015
First Time Home Buyers Credit (FTHBC)	Yes	03/30/2016	Yes	07/14/2015
Get Transcript (GETTRANS)	Yes	03/30/2016	Yes	07/14/2015
Health Coverage Tax Credit (HCTC)	Yes	05/06/2016	Yes	12/27/2017
Enterprise level, web-based data Tracking (eTRAK)	Yes	03/18/2016	Yes	01/18/2018
Excise Files Information Retrieval System (EXFIRS)	Yes	01/13/2017	Yes	04/19/2017
Excise Summary Terminal Activity Reporting System (ExSTARS)	Yes	01/13/2017	Yes	04/19/2017
Remittance Strategy for Paper Check Conversion (RSPCC)	Yes	09/23/2016	Yes	01/04/2018

Remittance Transaction Research (RTR)	Yes	05/26/2015	Yes	01/04/2018
Service Wide Employment Tax Research System (SWETRS)	Yes	01/26/2016	Yes	12/20/2017
Totally Automated Personnel System (TAPS)	Yes	10/05/2017	Yes	05/01/2017
Transcript Delivery System (TDS)	Yes	11/03/2015	Yes	03/22/2017
Tax Litigation Counsel Automated Tracking System (TLCATS)	Yes	05/04/2016	Yes	11/20/2017
TIN Matching (TM)	Yes	11/03/2015	Yes	03/22/2017
Tax Identification Number (PTIN) System (TPPS)	Yes	03/09/2017	Yes	03/29/2017
Web-Based Employee Technical Time System (WEBETS)	Yes	10/22/2015	Yes	12/05/2016
Withholding Compliance System (WHCS)	Yes	04/24/2015	Yes	08/24/2017
Where's My Amended Return (WMAR)	Yes	03/30/2016	Yes	07/14/2015

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

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

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

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

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

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. 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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Tax Return Database (TRDB)	Yes	11/06/2015	Yes	12/11/2012
Enterprise Directory Agent (EDA)	Yes	03/03/2017	Yes	05/31/2016
Individual Return Master File (IRMF)	Yes	03/09/2017	Yes	10/22/2015

Identify the authority and for what purpose? Tax Return Data Base (TRDB) - SAAS sends a list of employee TINS (sent as Tickler Files) to provide back related restrict TIN information on covered relationships for TIGTA reviews. Enterprise Directory Agent (EDA) - SAAS provides EDA read access to look at employee restricted tins (SEID Lookup table and restricted TIN Table) to verify Negative TIN role in EUP (Own/Spouse/Former Spouse). The process compares the EDA Negative TIN table stored on the Negative TIN Mainframe repository with TIN restrictions available in the SAAS Data Warehouse. New restrictions found in SAAS (limited to Spouse and former spouse) for users currently assigned to an EUP Negative TIN Role are added to the EDA Negative TIN Table. Individual Return Master File (IRMF) - SAAS sends a List of Employee SSN to IRMF as a 'Tickler' file so that they return us the bi-annual Outside Employer Restricted TINS

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

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

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

12e. 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, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.
While SAAS cannot verify that the applications that send audit data to SAAS provide users a notification, SAAS does display a Privacy Notice for all users of SAAS indicating that Use of the system consents to monitoring, and etc. The following is displayed: *****THIS U.S. GOVERNMENT SYSTEM IS 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 subjected to criminal and civil penalties. ****

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? The SAAS application only collects data from individual applications for auditing purposes.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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	Read-Only
Developers	Yes	Read-Only

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.	No		
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? Individuals have to submit an OL5081 request for access. Access is approved by the ESAT/SAAS PMO.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

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

22a. 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.

The National Archives and Records Administration (NARA) approved the destruction of SAAS Audit Data when 7 years old (Job No. N158-10-22, approved 4/5/2011). SAAS retention requirements are published under IRS Document 12990/Records Control Schedule 19 for Martinsburg Computing Center, item 88.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23.1 Describe in detail the system s audit trail. UserID, Usertype, System, EventType, EventID, TaxfilerTIN, SessionID, ScrAddr, ReturnCode, ErrorMsg, TimeStamp, VarData(Payload), TaxPeriod, MFTCode, ReturnType, TaxfilerTINType

J. PRIVACY TESTING

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

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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?
IRM Software Testing Standards and Procedures IRM 2.127 IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance OS:CTO:ES:EST:TS:TS-TMP-System-Test-PlanV1.4-10302014 template. All SAAS project assets are stored in the DocIT repository. Note: Test Documentation includes the artifacts and work products that provide evidence of successful verification of requirements. The End of Test Completion Report (EOTCR) will contain the summary results of all tests.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? 1.2 Test Summary of the SAAS Test Plan identifies all tests performed during the release for effective system validation and verification. IRM Software Testing Standards and Procedures IRM 2.127 IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance OS:CTO:ES:EST:TS:TS-TMP-System-Test-PlanV1.4-10302014 template. All SAAS project assets are stored in the DocIT repository. Note: Test Documentation includes the artifacts and work products that provide evidence of successful verification of requirements. The End of Test Completion Report (EOTCR) will contain the summary results of all tests.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

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

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes,** provide the date the permission was granted. 3/5/2015
If **no**, explain why not.

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: More than 100,000
26b. Contractors: Under 5,000
26c. Members of the Public: More than 1,000,000
26d. 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 9/11 Commission Recommendations 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. Application Audit Trails

N. ACCOUNTING OF DISCLOSURES

30. 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

If **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

30b. If **N/A**, explain the Exemption and/or Disclosure s response. Disclosures to Treasury for Tax Administration wouldn't require a record of accounting per IRC §6103(h)(1).

End of Report