

Date of Approval: July 14, 2015

PIA ID Number: **1405**

---

**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 and Analysis System PIA 6.18.2015 145357344

Next, enter the **date** of the most recent PIA. 11/9/2012

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 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.

**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 variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes On Primary Yes On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) 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 Preparer Taxpayer Identification Number (PTIN)

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

N/A

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
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
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
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)	Documents that have been marked OUO or LOU
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)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>Yes</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>Yes</u>	PII for personnel administration is 5 USC
<u>Yes</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>Yes</u>	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 variations) 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**

Treas/IRS 34.037 Audit Trail and Security Records System

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. N/A

---

**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.

<b><u>System Name</u></b>	<b><u>Current PIA?</u></b>	<b><u>PIA Approval Date</u></b>	<b><u>SA &amp; A?</u></b>	<b><u>Authorization Date</u></b>
IFS	Yes	09/10/2014	Yes	03/04/2015
IMS	Yes	09/12/2013	Yes	04/20/2015
MEF	Yes	12/17/2014	Yes	01/07/2015
Mod-IEIN	Yes	06/16/2010	Yes	09/09/2010
OPA	Yes	04/07/2010	Yes	06/09/2010
AMS	Yes	12/02/2014	Yes	05/13/2015
AUR	Yes	07/12/1913	Yes	10/01/2014
IPS	Yes	07/02/2014	Yes	09/25/2012
WHCS	Yes	04/24/2015	Yes	01/09/2013
CDE	Yes	04/25/2013	Yes	02/05/2015
EAUTH	Yes	01/29/2013	Yes	11/25/2014
ITIN-RTS	Yes	02/17/2015	Yes	09/20/2012
RCCMS	Yes	01/08/2015	Yes	03/22/2013
RICS	Yes	06/02/2014	Yes	02/01/2012
RTR	Yes	05/26/2015	Yes	11/28/2012
TDS	Yes	06/28/2013	Yes	08/28/2013
AUTH TTPS	Yes	11/10/2011	Yes	08/25/2011
EFP-Help	Yes	06/28/2013	Yes	08/20/2013
FSA-D	Yes	06/28/2013	Yes	08/28/2013
AFOIA	Yes	11/13/1914	Yes	05/30/2012

BDA	Yes	09/10/1914	Yes	11/26/2012
ETRAK	Yes	04/29/2014	Yes	04/20/2012
EXSTARS	Yes	02/26/2014	Yes	06/13/2011
FATCA	Yes	12/02/2014	Yes	11/26/2013
FTHBC	Yes	06/28/2013	Yes	08/28/2013
FATCA ICMM-FIR	Yes	12/02/2014	Yes	11/26/2013
E-Services	Yes	12/06/2013	Yes	02/28/2014
Ex-FIRS	Yes	02/26/2014	Yes	06/13/2011
EAIB	Yes	04/10/2010	Yes	11/15/2011
EMP REG	Yes	04/29/2010	Yes	11/15/2011
RSPCC	Yes	09/29/2010	Yes	02/11/2011
ICCE	Yes	06/28/2013	Yes	08/28/2013
TM	Yes	12/06/2013	Yes	02/28/2014

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

---

#### F. PII SENT TO EXTERNAL ORGANIZATIONS

---

12. Does this system disseminate SBU/PII? 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, cloud, 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 can't 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

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

Contractor Employees? Yes

<u>Contractor Employees?</u>	<u>Yes/No</u>	<u>Access Level</u>	<u>Background Invest.</u>
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 asking for access. Access is approved by the ESAT 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. N1-58-10-22, 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

23a. If **yes**, what date was it completed? 5/12/2015

23.1 Describe in detail the system s audit trail. UserID UserType System EventType EventID TaxfilerTIN SessionID SrcAddr ReturnCode ErrorMsg TimeStamp VarData (Payload) TaxPeriod MFTCode Return Type 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?

1.2 Test Summary of the SAAS Test Plan Identifies all tests performed during the release for effective system validation and verification.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements 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-Plan-V1.4-10302014 template All SAAS project assets are stored on DocIT at: <http://nct0010cp642188/docit/drl/objectId/0b007562804e787f> 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

25b. If **yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

---

**L. NUMBER AND CATEGORY OF PII RECORDS**

---

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

26a. IRS Employees:	<u>More than 100,000</u>
26b. Contractors:	<u>Under 5,000</u>
26c. Members of the Public:	<u>More than 1,000,000</u>
26d. Other:	<u>No</u>

---

**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? No

---

**End of Report**

---