REQUEST FOR RECORDS DISPOSITION AUTHORITY *(See Instructions on reverse)*	LEAVE BLANK (NARA use only) JOB NUMBER **N1-58-10- 22**
TO NATIONAL ARCHIVES and RECORDS ADMINISTRATION (NWML) 8601 ADELPHI ROAD, COLLEGE PARK, MD 20740-6001	DATE RECEIVED 8/31/10
1 FROM (Agency or establishment) Department of the Treasury 2 MAJOR SUBDIVISION Internal Revenue Service 3 MINOR SUBDIVISION	NOTIFICATION TO AGENCY In accordance with the provisions of 44 U S C 3303a the disposition request, including amendments, is approved except for items that may be marked "disposition not approval" or "withdrawn" in column 10
4 NAME OF PERSON WITH WHOM TO CONFER Tracee Taylor (REFM-Records) Michael L Jenkins (SAAS PM) 5 TELEPHONE 202-435-6308 202-283-1170	DATE 5/Jun 11 ARCHIVIST OF THE UNITED STATES

5 AGENCY CERTIFICATION

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached 3 pages(s) are not now needed for the business of this agency or will not be needed after the retention periods specified, and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies,

[redacted] is not required, [redacted] is attached, or [redacted] has been requested

DATE	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE
8/26/2010	Daniel W Bennett IRS Records Officer	IRS Records Officer National Office, OS A RE L RIM Washington, DC 20224

7 ITEM NO	8 DESCRIPTION OF ITEM OF PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	RCS 1.15.19, *Records Control Schedule for Martinsburg Computing Center* **Update:** **1 15.19 New Item 88, Security Auditing and Analysis System (SAAS)** **(see attached)**		

REQUEST FOR RECORDS DISPOSITION AUTHORITY (See Instructions on reverse)		LEAVE BLANK (NARA use only) JOB NUMBER N1-58-10-	
1	**1.15 19 New Item 88, Security Auditing and Analysis System (SAAS)** **Background:** *The purpose of the Security Audit and Analysis System (SAAS) 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* *SAAS implements a data warehousing solution to provide on-line analytical processing of audit trail data The system enables the IRS and TIGTA to detect potential unauthorized accesses to IRS systems and enables users to analyze and report on audit log data for both Modernized and Current Processing Environment (CPE) applications The audit trail consists of a standardized record and is flexible enough to capture all events of audit interest All audit trail records generated from any source within the modernized infrastructure are available for capture and analysis in the SAAS Data Warehouse* *IDRS audit trails are transferred from two computing centers, which house data from all 10 service centers and loaded into the SAAS Data Warehouse also on a daily basis Operational system and security logs that are generated by business applications and Internet Security System (ISS) infrastructure applications are sent to the Log File Collector (LFC) and selected audit logs are forwarded to SAAS via the Tivoli Data Mover on a daily basis* *SAAS collects, stores, and reports audit trail data for the investigation of instances of Unauthorized Access (UNAX) violations against IRS computer systems SAAS collects log data at both the network and application layer, specifically, log data from the core services and Web Hosting environments Audit logs can be generated from any source and captured and analyzed in the audit data warehouse The queries associated with SAAS reports allow managers, security, and law enforcement personnel to audit the actions of IRS employees on IRS systems by their standard employee identification number (SEID) Audit data indicates the dates and times employees are logged in and what data they have accessed* *SAAS is comprised of four modules Infrastructure, Modernized, IDRS, and Criminal Investigation (CI), which allows users to review audit trails with different reporting capabilities* *Authorized and authenticated SAAS users can access data through authorized reports and queries* *SAAS end users and SAAS administrators are registered for roles per their specific user group (i e , TIGTA, Computer Security Incident Response Center [CSIRC], CI, and MITS) and can only view and generate reports* *The user's manager or the Business Owner of the respective SAAS module determines who has access to SAAS This determination is based on the individual's defined duties and*		

corresponding role(s) To gain access to SAAS, all potential users have their user roles established, which identifies specific reports and queries that they are authorized to access

Description:

The Security Audit and Analysis System (SAAS) enables the IRS and TIGTA to detect potential unauthorized accesses to IRS systems and enables users to analyze and report on audit log data for both Modernized and Current Processing Environment (CPE) applications

a. Inputs:

SAAS receives receives weekly feeds of employee and taxpayer ancillary data from Information Returns Master File Processing (IRMF), and bi-annual data feeds from IRMF including restricted spouse employer and outside employer TINs

GRS 20.2

SAAS receives daily data feeds from Corporate Authoritative Directory Service (CADS) that update the SAAS Standard Employer Identifier (SEID) look-up table

SAAS receives daily application audit trails from Account Management System (AMS), Compliance Data Environment (CDE), E-Services, Individual Taxpayer Identification Number-Real Time System (ITIN-RTS), Integrated Data Retrieval System (IDRS), Integrated Financial System (IFS), Internet Refund-Fact of Filing (IRFOF), Modernized e-File (MeF), Modernized Internet Employer Identification Number (Mod-IEIN), Online Payment Agreement (OPA), Remittance Strategy-Paper Check Conversion (RS-PCC), Risk Based Scoring System (RBSS), Reporting Compliance Case Management System (RCCMS), Electronic Filing PIN-Help (EFP-Help), and Federal Student Aid Datashare (FSA-D)

Disposition: Temporary Delete/Destroy any cached input files and data immediately following validation of receipt by the system

b. System Data (Master Files)

SAAS collects and stores log data at both the network and application layer, specifically, log data from the core services and Web Hosting environments SAAS is comprised of four modules Infrastructure, Modernized, IDRS, and Criminal Investigation (CI) which allows users to review audit trails with different reporting capabilities Audit data includes a mix of taxpayer and IRS employee data, including taxpayer name, address and TIN, dates and times employees are logged in and what data they have accessed, restricted TIN list for an employee, event ID and type, time stamp, session ID, user ID and type, error message or code, and source address

Disposition: Temporary Delete/Destroy after 7 years Maintain data online for 6 years, maintain data near line for an additional year, then delete

c Outputs:

The queries associated with SAAS reports allow managers, security, and law enforcement personnel to audit the actions of IRS employees on IRS systems by entering a Taxpayer TIN, Employee SSN, or Employee standard employee identification number (SEID) The audit trail consists of a standardized record and is flexible enough to capture all events of audit interest

GRS 20 5

Disposition Temporary Destroy when no longer needed for audit or operational purposes, whichever is later

d System Documentation

exception to GRS 20.11

Includes date system specifications, codebooks, records layout, and user guide

Disposition: Temporary Delete/Destroy when superseded or 5 years after the system is terminated, whichever is sooner