

NOTE: The following reflects the information entered in the PIAMS Website.

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: 04/02/2014 PIA ID Number: 808

---

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

---

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

CI-1 GSS

---

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

---

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Under 100,000

---

4. Responsible Parties:

NA

---

5. General Business Purpose of System

---

Criminal Investigation (CI) serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law. The CI-1 GSS is integral in supporting the mission of CI as the GSS provides network connectivity to internal CI applications Criminal Investigation Management Information System (CIMIS), Public Information Officer Database (PIOner), and other IRS applications such as the Integrated Data Retrieval System (IDRS). The CI network provides users with the necessary infrastructure to access e-mail services, file services, print services, and access to management and inventory database systems. The network operates on top of the IRS wide area network (WAN) with CI local area network (LAN) segments isolated behind CI routers for additional layer of security. Due process is provided outside of the system pursuant to 26 USC and 18 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact \*Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 11/30/2010

---

6b. If Yes, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) Yes
  - System is undergoing Security Assessment and Authorization Yes
- 

6c. State any changes that have occurred to the system since the last PIA

NA

---

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

---

## B. DATA CATEGORIZATION

---

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems Yes  
Employees/Personnel/HR Systems Yes

Other Yes

*Other Source:*

Employee Investigative Work  
Product related to Criminal  
Investigation and  
Surveillance, Legal  
Investigation, Substance  
Control, Judicial Hearings,  
and Grand Jury.

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	Yes
Tax Payer ID Number (TIN)	Yes	Yes	Yes
Address	Yes	Yes	Yes
Date of Birth	Yes	Yes	Yes

Additional Types of PII: Yes

PII Name      On Public? On Employee?  
Any from Investigations No      No

10a. Briefly describe the PII available in the system referred to in question 10 above.

Anything potentially related to Criminal Investigations.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

Employee Information, such as personnel, payroll, and evaluation data. All taxpayer related information covered by § 6103 of the Internal Revenue Code. Name, Home address, Social Security number, Date of birth, Home telephone number, PII.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

N/A

---

**10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?**

CI-1 adheres to the security requirements defined in NIST SP 800-27 and IRM 10.8.1. In addition, continuous monitoring is performed annually to ensure the application continues to meet FISMA security requirements.

**11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.**

The following data types are collected in the Audit Trail: -Date/Time Stamp (The Date/Time of when the Audit Record was created) -Unique Identifier (The Unique Identifier that initiates the action for the audit record, such as the user name or SID) -Event Type (The Event Type field is used to track the type of event that is executed such as create, update, or delete) -Origin of Request (The origin of where the request was made, such as the Terminal ID) -Name of Object (The name of the object that was introduced, accessed, or deleted) -User Identity (The identity of the user who performed the action) -User Role (The role of the user at the time the action was performed)

**11a. Does the Audit Trail contain the audit trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes**

---

**12. What are the sources of the PII in the system? Please indicate specific sources:**

**a. IRS files and databases: Yes**

If Yes, the system(s) are listed below:

No System Records found.

**b. Other federal agency or agencies: Yes**

If Yes, please list the agency (or agencies) below:

Every federal and state agency is a potential source, and every county and state is a potential source. Therefore, the CI-1 GSS has thousands of sources, so it is not feasible to list every potential source to the CI-1 GSS. Any local, municipality county, state, or federal information source is a potential information source.

**c. State and local agency or agencies: Yes**

If Yes, please list the agency (or agencies) below:

Every federal and state agency is a potential source, and every county and state is a potential source. Therefore, the CI-1 GSS has thousands of sources, so it is not feasible to list every potential source to the CI-1 GSS. Any local, municipality county, state, or federal information source is a potential information source.

**d. Third party sources: Yes**

If yes, the third party sources that were used are:

Every federal and state agency is a potential source, and every county and state is a potential source. Therefore, the CI-1 GSS has thousands of sources, so it is not feasible to list every potential source to the CI-1 GSS. Any local, municipality county, state, or federal information source is a potential information source. As well as privately owned information such as banks.

**e. Taxpayers (such as the 1040): Yes**

**f. Employees (such as the I-9): Yes**

**g. Other: Yes If Yes, specify: Any that could yield Criminal Investigation data.**

---

**C. PURPOSE OF COLLECTION**

*Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use*

**13. What is the business need for the collection of PII in this system? Be specific.**

Use in investigations as it relates to criminal activity.

---

**D. PII USAGE**

*Authority: OMB M 03-22 & PVR #16, Acceptable Use*



---

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent \_\_\_\_\_

Website Opt In or Out option \_\_\_\_\_

Published System of Records Notice in the Federal Register \_\_\_\_\_

Other: \_\_\_\_\_

---

## G. INFORMATION PROTECTIONS

---

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>Read Write</u>
Developers		<u>No Access</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>Read Write</u>
Contractor System Administrators		<u>Read Write</u>
Contractor Developers		<u>No Access</u>
Other:	<u>No</u>	

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level" background investigation? Yes

23. How is access to the PII determined and by whom?

Based on a user's position and need-to-know, the manager determines access to the data. The manager will request that a user be added. They must fill out Form 5081, Information System User Registration/Change Request, to request access to the application. A user's access to the data terminates when it is no longer required. Criteria, procedures, controls, and responsibilities regarding access are documented in the Information Systems Security Rules on Form 5081.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

CI-1 is the General Support System for CI consisting and as such does not in itself have data input to maintain. The accuracy, completeness, validity, and authenticity are done at the application-level and are referenced in the application PIAs. At the application level "Different levels of CI Management are responsible for reviewing data

entries. Periodic reviews and inventories are conducted specifically to measure the accuracy, timeliness and completeness of data entered. The applications enforce data entry field restrictions through business rules. CI personnel are also responsible for the accuracy of data they input into the applications.

---

**25. 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**

---

**25a. 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.**

CI-1 General Support System (GSS) is non-recordkeeping. It provides infrastructure support and data security to servers that host CI-related applications. Disposition instructions for CI recordkeeping systems are published under IRM 1.15.30 (soon to transition to Records Control Schedule (RCS) Document 12990, under RCS 30) for Criminal Investigation Records, and/or RCS 20 for Administrative/Organization Support Operational Records (already published in Document 12990).

**If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.**

---

**26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.**

CI-1 adheres to the security requirements defined in NIST SP 800-27 and IRM 10.8.1. In addition, continuous monitoring is performed annually to ensure the application continues to meet FISMA security requirements.

**26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.**

CI-1 adheres to the security requirements defined in NIST SP 800-27 and IRM 10.8.1. In addition, continuous monitoring is performed annually to ensure the application continues to meet FISMA security requirements.

---

**27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes**

---

**28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.**

In accordance with IRM 10.8.1 and NIST SP 800-37, continuous monitoring activities (including configuration management and ongoing annual testing of security control) are performed for IRS general support systems and applications. Testing is accomplished by selecting an appropriate subset of controls for testing for each system. The subset of controls is selected based on the controls for POA&M items that have been completed, and controls deemed to have high volatility (i.e., have the greatest potential for change after implementation).

---

**29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Yes**

---

**29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? Yes**

**29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? 01/01/2014**

---

## **H. PRIVACY ACT & SYSTEM OF RECORDS**

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to \$5000.

*Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency*

---

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

---

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

**SORNS Number**

**SORNS Name**

Treas/IRS 46.002 Criminal Investigation Management Information

Treas/IRS 46.009 Centralized Evaluation and Processing of Informati

Treas/IRS 46.022 Treasury Enforcement Communications System

Treas/ IRS 46.050 Automated Information Analysis System

Treas/IRS 34.037 IRS Audit Trail and Security Records system

**Comments**

**I. ANALYSIS**

---

*Authority: OMB M 03-22 & PVR #21- Privacy Risk Management*

---

**32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?**

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

**32a. If Yes to any of the above, please describe:**

NA

[View other PIAs on IRS.gov](#)