DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

COMMUNICATIONS AND LIAISON

MEMORANDUM FOR JIM STRICKLIN DIRECTOR, WEB SERVICES

FROM: Maya A. Bernstein Charlene W. Evans
Privacy Advocate

SUBJECT: WEB Services Registered User Portal
Privacy Impact Assessment

The Office of the Privacy Advocate has reviewed the Privacy Impact Assessment (PIA) for the WEB Services Registered User Portal (RUP) project. Based on the information you provided, our office does not have any privacy concerns that would preclude RUP from operating. However, a revised PIA is required when considering any future upgrades or major modifications or at the scheduled recertification of this system.

We are forwarding s copy of the PIA to the Director of the Security Services Mission Assurance Certification Program Office, to be included in the Security Accreditation Package for formal acceptance for operation. We are also forwarding a copy to the Director, Security Policy Support and Oversight, who may request information concerning the statements contained in the PIA to ascertain compliance with applicable security requirements.

If you have any questions please contact me at 202-927-5170, or your staff may contact Gino Talbot at 202-622-2302.

Attachment

cc: Director, Security Services Mission Assurance, Certification Program
Office M:S:A
Director, Security Policy Support and Oversight M:S:S

Appendix B
Registered User Portal (RUP) Infrastructure Components

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories: A. Taxpayer B. Employee C. Audit Trail Information (including employee log-in info) D. Other (Describe)	Data elements (Table 1) requested or retrieved via the messaging subsystem (AMDAS) are logged to the Security Audit and Analysis System (SAAS) for the purpose of auditing. The data elements that are brought into the system are marked with an asterisk in the attached Table 1. A. Taxpayer Identification Numbers (TIN) are recorded to identify specific record access. B. Employee numbers are recorded when accessing taxpayer information. Reference line item #3 & 26 in the data elements table #1. C. Information is stored and maintained in the SAAS system accessible by the Computer Security Incident Response Center (CSIRC) and the Treasury Inspector General for Tax Administration (TIGTA) personnel for the purpose of reviewing audit trails. The SAAS system will store queried information for UNAX analysis on who did what, when they did it, and what records were accessed. D. N/A

Appendix B
Registered User Portal (RUP) Infrastructure Components

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources. A. IRS B. Taxpayer C. Employee D. Other Federal Agencies (List agency) E. State and Local Agencies (List agency) F. Other third party sources (Describe) RUP is for Internet access by third parties. Employee access is via EUP.	A. IRS authorized personnel access audit records. Audit records include time, date, requested action, results and application request. (For specific elements of each application please reference the IEIN, and the IRFOF PIAs). B. NONE C. User accounts are maintained that contain employee identification information to track employees that administer the RUP. D. NONE E. NONE F. NONE
3. Is each data item required for the business purpose of the system? Explain.	Yes- The data items are required for UNAX analysis and logging procedures.
4. How will each data item be verified for accuracy, timeliness, and completeness?	Regular reviews and Audits are performed by the Treasury Inspector General for Tax Administration (TIGTA), and the Computer Security Incident Response Center (CSIRC) personnel to ensure proper operation and accuracy of the information. Also it's the system's Information System Security Officer's (ISSO) duty to review information for accuracy on a regular basis.
5. Is there another source for the data? Explain how that source is or is not used.	No- Each request must be captured and logged as it is received or processed.
6. Generally, how will data be retrieved by the user?	Log data is accessed via the SAAS system that store the audit trail by authorized TIGTA or CSIRC personnel

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?	Yes. TINs are stored for audit purposes to identify what records were accessed. Unique employee identifiers are stored to identify who accessed the corresponding TIN.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?	TIGTA Auditors and entire CSIRC organization Will have access to the audit information on the SAAS system.
9. How is access to the data by a user determined and by whom?	I.A.W IRM 25.10.1.3.11 a 5081 is required to access the data. Business Owner determines those authorized. The user's Managers are responsible for granting and revoking user's accesses as necessary.
10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared. If NO, continue to Question 12.	YES – Any AMDAS captured information is sent to SAAS via AMDAS setup.
11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?	YES - The SAAS system within the STIR – ISS infrastructure has a Certification for
12. Will other agencies provide, receive, or share data in any form with this system?	YES – TIGTA is a Treasury organization.

Appendix B
Registered User Portal (RUP) Infrastructure Components

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?	No – The WEB Registered User Portal system does not use persistent cookies, session cookies are captured for user authentication purposes only. Session cookies are released at the end of the current web session.