Date of Approval: **October 27, 2021**

PIA ID Number: **6374**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Web-Based Employee Technical System, WebETS

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Web-Based Employee Technical System, WebETS, 4B, 3693

What is the approval date of the most recent PCLIA?

10/1/2018

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Tax Exempt & Government Entities (TE/GE) Investment Executive Steering Committee (IESC)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Operations & Maintenance (i.e., system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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 Tax Exempt and Government Entities (TE/GE) Division of the Internal Revenue Service (IRS) uses a time reporting system to track the use of its resources in meeting business objectives. The WebETS system provides TE/GE employees a web-based application to record time and manage their inventory as it is applied to each case/activity. As work plan data is developed at the executive level, each division of TE/GE uses the data to monitor the effective use of its resources. All reports produced by WebETS are internal management reports within TE/GE.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Interfaces with external entities that require the SSN

Legal/statutory basis (e.g., where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

When establishing inventory on the system, agents enter the name and identifying information for each return/case. In very limited instances this might include an individual names and SSN, but generally would be the organization or employee plan name and EIN. The name, SEID and organizational information of employees (including group number) is maintained in the application tables for account access and to ensure proper reporting of functional time spent.

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

There is no current mitigation planned due to the limited instances in which an SSN is used. When establishing inventory on the system, agents enter the name and identifying information for each return/case. In very limited instances this might include an individual names and SSN, but generally would be the organization or employee plan name and EIN. The name, SEID and organizational information of employees (including group number) is maintained in the application tables for account access and to ensure proper reporting of functional time spent.

Employer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e., names, addresses, etc.)?

Yes

Specify the PII Elements:

Name
E-mail Address
Standard Employee Identifier (SEID)
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

SSN for tax returns and return information is Internal Revenue Code Section 6109

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

When establishing inventory on the system, agents enter the name and identifying information for each return/case. In very limited instances this might include an individual names and SSN, but generally would be the organization or employee plan name and EIN. The name, SEID and organizational information of employees (including group number) is maintained in the application tables for account access and to ensure proper reporting of functional time spent.

How is the SBU/PII verified for accuracy, timeliness, and completion?

SBU/PII is verified manually by the manager for accuracy, timeliness, and completeness. WebETS does NOT make determinations. All determinations are completed through the Examination, Rulings and Agreement process with no direct correlation to WebETS.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 34.037 Audit Trail and Security Records

IRS 50.222 Tax Exempt/Government Entities (TE/GE) Case Management Records

IRS 36.003 General Personnel and Payroll Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Corporate Authoritative Directory Service (CADS)
Current PCLIA: Yes
Approval Date: 9/18/2020
SA&A: Yes
ATO/IATO Date: 1/3/2020

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Security Audit & Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2020

Identify the authority.

Internal Revenue Code sections 6001, 6011, 6057, and 6058

For what purpose?

Security Audit and Analysis System (SAAS) - web application activity is sent to SAAS for security auditing purposes.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Notice, consent, and due process are provided pursuant to 5 USC.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for. Their response is mandatory under these sections." WebETS is a time tracking system used by TE/GE to record time and manage inventories and monitor resources expended.

How does the system or business process ensure 'due process' regarding information access, correction, and redress?

Notice, consent, and due process are provided pursuant to 5 USC.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

How is access to SBU/PII determined and by whom?

The employee's manager and account administrators for WebETS approves entitlement access requests via BEARS. Employees only have access to their own inventory. Managers only have access to the employees and inventory within their group.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

Paper-based retentions for Employee Plans, Exempt Organization Application Case Files are covered under Internal Revenue Manual (IRM) 1.15.24 Records Control Schedule (RCS) for Tax Administration - Tax Exempt and Government Entities. WebETS requires deletion of data 7 years after the fiscal year cutoff and deletion of aging data reports 5 years after the fiscal year cutoff. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. RCS 24 Items 76-Web-Based Employee Technical Time System (WebETS) and 77 Aging Data Report.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

1/6/2021

Describe the system's audit trail.

The following data elements are collected in the Web-ETS audit trail: Date time stamp (e.g., date and time of the event); Unique identifier (e.g., username, SEID, Application name, or application initiating the event); Type of event; Origin of the request (e.g., terminal ID) for identification/authentication of events; Name of object introduced, accessed, or deleted from a user's address space; -Role of user when creating the event; and Success/Failure of the event.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

WebETS uses the Corrective path for Enterprise Life Cycle (ELC) purposes. Per the ELC Tailoring Table, a System Test Plan is not required for the Corrective path.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

7/21/2015

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: 100,000 to 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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