Date of Approval: **February 09, 2021**

PIA ID Number: **5837**

SYSTEM DESCRIPTION

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

Investigative Workstations, IW

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?

PCLIA (v.2) 3247

What is the approval date of the most recent PCLIA?

2/9/2018

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.

SBSE Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

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

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

No

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 Investigative Workstations (IW) will be used by Revenue Agents assigned to the Small Business/Self Employed (SB/SE) Lead Development Center (LDC) to perform case development on leads in process; identify new leads; or at the request of Abusive Transaction (AT) Revenue Agents assigned approved IRC 6700/6701 investigations. These computers have a very restricted and limited use policy and should not be used for any other reason than their original intent which is to assist the LDC and the AT field research requests. In developing their assigned lead, the LDC RA will conduct internet research to determine if the subject has a presence on the internet and capture relevant evidence such as websites, business Facebook pages or business filings with State Secretary of State websites. At a minimum, LDC RA's should determine if the subject: Utilizes a website or social media to promote their tax preparation business or tax avoidance scheme. Is making tax-related representations on internet newsgroups, blogs and social media. Research performed at the request of AT RA's assigned approved IRC 6700/6701 investigations must be approved by the LDC Group Manager before assigned to the LDC Revenue Agent. Once the information has been captured on the IW computer, it will be scanned for Viruses using Norton software and then will be burned to a disc. The information will either be incorporated in the case file of the lead under development or sent electronically to the Revenue Agent who requested it. To ensure protection of Civil Liberties, Internal Revenue Service (IRS) employees may only request information that is pertinent for tax administration for specifically assigned cases. The IWs are monitored to prevent unauthorized access.

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.)?

No

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

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Internet Protocol Address (IP Address)

Criminal History

Certificate or License Numbers

Biometric Identifiers

Employment Information

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

No

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

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

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.

Investigative Workstations allow taxpayer internet research outside of IRS firewalls, and do not leave behind an IRS footprint. This will reduce the possibility that the subject will remove critical evidence posted to the internet if IRS visitations to their website are detected. Also, many tax practitioners maintain a Business Facebook page in lieu of a website and the evidence contained on these social media pages would not be accessible through the IRS network due to the filters in place. The IW will be used to access and download information that is publicly available via the Internet. This may involve capturing the taxpayer's web site, business Facebook Page, corporate filings with the State Secretary of State office, or any other information that is germane to the subject under consideration for a IRC 6700/6701 investigation (or has already been approved for a IRC 6700/6701). Occasionally, the individual with dominion and control over a website making abusive tax shelter claims is not disclosed on the website. When the content appears potentially actionable under IRC 6700/6701, the LDC RA may conduct research which could lead to the identity of the principal behind a website by searching Internet Corporation for Assigned Names and Numbers (ICANN) (URL: internic.net) website by the domain name (such as "badpreparer.com"). Once the Domain name registrar has been identified, the LDC Revenue Agent can go to their website and query their "Who Is" directory and the registrant should be listed unless the registrant elected "Private" registration. The LDC RA also may ascertain who the hosting entity is for the promoter's website through though the American Registry for Internet Numbers (ARIN) website. Also, research may be done at the request of DOJ to support cases that have been referred for possible civil actions which may lead to an injunction or a finding of contempt if the subject has violated a court order. Complaints posted on Yelp may indicate that a practitioner may be violating a court order by continuing to prepare returns after the date of a court order barring the preparer from doing so. Internet searches conducted by LDC Revenue Agents may include name, address, phone number, and DBA or name of associated business. Social Security Numbers should not be used in any IW queries. The data will be saved to a CDR and any saved data will be manually deleted from the workstation. The data on the CDR will be uploaded to the LDC RA's laptop and the CDR destroyed. The data will then be included in the electronic file or transmitted to the requesting AT RA. TIGTA in a report issued in April 2004 entitled "The Lead Development Center Effectively Researched Abusive Tax Scheme Leads but Could Be More Proactive in Identifying Promoters" (Reference Number: 2004-30-087), recommended that " the LDC becomes more proactive in researching the Internet to independently identify promoters of abusive tax schemes." The business needs include a means to document web sites in a manner presentable in court; improved hardware and software, which will increase efficiency of existing searches, and in the identification of tax scheme promoters and preparers. LDC RA's recognizes once information from the public site is input into an IRS record/computer for purposes of tax administration, that record becomes subject to confidentiality protections of IRC 6103, and for records retrieved by individual identifier (i.e. an ATAT promoter) by the Privacy Act.

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

In most cases, web sites will be captured as completely as possible with the Revenue Agent using an Advanced Google Search to identify pages that may not be apparent by spidering (tracing through) the links of the individual web pages. Every attempt is made to present the information captured as accurately as the software will allow which in most cases will be exactly as the public views them. In some cases, web pages which deploy multiple frames or certain scripts will not capture accurately using our web capture software (Snagit) or through a pdf save. In those cases, the Revenue Agent will have to take screen shots of these web pages with some pages requiring multiple screen shots to capture the entire page from top to bottom which are then pasted in a word document in sequential order and saved as a pdf file. All web captures should include all text and graphic elements in their original arrangement. Also, the URL of each web page captured should be recorded as well as the date of the capture and the person making the capture. As explained in Policy Statement 1-236, Fairness and Integrity in Enforcement Selection, IRS employees are expected to carry out our duties with integrity and fairness. Towards that end, IRM Section 4.32.2.4.2 provides that: To ensure fairness to the taxpaying public, our Examination Workplan provides a balanced approach for return delivery and allocation of resources to address areas of the Tax Gap by taking into account factors such as income levels, geographic locations, and return types. To ensure an equitable process for all promoters and preparers, selection decisions are made utilizing available experience and/or statistics indicating the probability of substantial error. No one individual can control the investigation selection decision-making process. We limit involvement to only those employees whose duties require them to be included. To ensure fairness to each promoter/preparer who is selected for IRC §6700/§6701 investigation, selection decisions are based on the underlying relevant tax law and the following criteria: -The promoter/preparer activity is abusive in nature. -Money is exchanged for products and services. -Potential harm to taxpayers. Managerial reviews of selection decisions occur during each phase of the selection and assignment process. SB/SE LDC will develop each lead independently using established criteria to either recommend or not recommend an IRC §6700/§6701 investigation: -Recommendation memos are reviewed by the LDC Group Manager and the LDC Program Manager. -Non-Recommendation memos are reviewed by the LDC Group Manager. -As part of the Program Review process, the Lead Development Center Program Manager (or designee) ensures the LDC Group Manager reviews adhere to the examination case selection policy.

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 42.021 Compliance Programs and Projects Files

IRS 34.037 Audit Trail and Security 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?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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.?

Yes

Briefly explain how the system uses the referenced technology.

The system may use maps to locate assets and may use biometric data such as name, age, date of birth, etc., to verify taxpayer assets, residence, business interest or other applicable information needed for the purposes of case disposition and resolution.

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?

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.

Information is not directly collected from individuals; it is collected from publicly available information on the Internet.

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

No

Why not?

The laptops access public records for research. There is no interaction with the public or with taxpayers.

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

The Taxpayer Bill of Rights publication 1 at http://core.publish.no.irs.gov/pubs/pdf/p1--2014-12-00.pdf outlines the baseline for 'due process' that business follows. Due process is not applicable to the public in general as the system does not "use" the event information to interact with the tax paying public in any way. IRS employees and contractors using IRS

email and web services may face disciplinary action for the misuse of SSNs. All IRS employees will be given the opportunity to defend their actions before a final determination is made. Contractor employees will be afforded any rights granted within the regulations that cover the specific contract they are working under.

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 Only

Managers: Administrator

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

Access to the IW is limited to Revenue Agents assigned to the Lead Development Center, as determined by the LDC Group Manager and Program Manager. The LDC has two standalone computers assigned to the unit. These computers have a very restricted and limited use policy and should not be used for any other reason than their original intent which is to assist the LDC and the AT field research requests.

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.

IW is non-recordkeeping. It is not the official repository for any data or documents and does not require a National Archives and Records Administration-approved records control schedule to affect data disposition. IW is used to facilitate the research and collection of case-related information publicly available on the Internet. No taxpayer information will be

stored on the computer. Information captured from the Internet will be downloaded and stored on a compact disk or other external storage media and associated, maintained in accordance with the taxpayer's administrative file. The retention period will follow existing procedures for retaining administrative files associated with a taxpayer's examination workpapers, Compliance Initiative Projects, and Collection case files. RCS 23 Item 1-Examination Subject Files- RCS 23 Item 2-Examination Subject-Numerical Files. RCS 23 Item 42-Examination Case Files. RCS 23 Item 72-Compliance Initiative Project Files. Destroy 3 years after termination. RCS 28 Item 6-Case Files.

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

Revenue Agents using the IW are required to complete a usage log detailing the date and time IW's were used, business reason for using the standalones (i.e., research to support a lead they are developing or research performed to support an approved IRC 6700/6701 investigation at the Request of the Revenue Agent assigned the case). The associated control number of the lead under development or approved for an IRC 6700/6701 investigation is also recorded in the log as well as a listing of websites visited during each session. These manual logs are reviewed by the Group Manager every month. Also, either the Program Manager or Group Manager will employ Cisco Umbrella Software to Remotely Monito internet usage.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Because the IW are standalone laptops which are not connected to any IRS system or server, a system test plan is not required.

SBU DATA USE

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

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: Not Applicable

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?

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.

The system will have the capability of monitoring business related websites, business related social media sites or other sites which might contain information relevant to developing a promoter lead or support an active investigation. Each request to capture a website must be approved by the Group Manager and there are no "open ended" monitoring requests. Cisco Umbrella Software to Remotely Monitor internet usage and will be used to monitor and audit the use of the laptops. There is no recognized limited personal use policy for the workstations and use of the workstation is strictly limited to Revenue Agents assigned to the Lead Development Center. Revenue Agents using the IW are required to complete a usage log detailing the date and time IW's were used, business reason for using the standalones (i.e.,

research to support a lead they are developing or research performed to support an approved IRC 6700/6701 investigation at the Request of the Revenue Agent assigned the case). The associated control number of the lead under development or approved for an IRC 6700/6701 investigation is also recorded in the log as well as a listing of websites visited during each session. These manual logs are reviewed by the Group Manager every month. Also, either the Program Manager or Group Manager will employ Cisco Umbrella Software to Remotely Monitor internet usage.

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