Date of Approval: June 21, 2016 PIA ID Number: **1646**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Light Client Technology Demonstration, LCTD

2. Is this a new system? Yes

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

Yes	Vision & Strategy/Milestone 0
Yes	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? No

A.1 General Business Purpose

5. 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 Light Client Technology Demonstration provides IRS IT and its business representatives with the knowledge and experience for future requirements and IT services delivery to the user. These devices will be leveraged as examples of light clients and used to host various tests of use case scenarios to determine capabilities and performance of this technology, as well as suitability for the IRS environment. Performing a technology demonstration utilizing light client devices is critical to IRS in fleshing out the proper requirements, expectations, and target use cases to validate direction and ensure the best strategic investments going forward. Light client capabilities can provide flexible alternatives to client computing services by allowing for certain bring your own (BYO) computer scenarios as well as extend the life of aging equipment. Additional potential use scenarios include: - Contractor workstation alternative - Light Client instead of full IRS loaner system - Disaster recovery - Light Client to boot off any available system during disaster - Equipment repair - Utilize a Light Client while IRS laptop/desktop is out of service - others not yet discovered USB devices will be utilized to demonstrate two modes of operation. - The first being to host a full, self-contained version of Windows on the portable USB device, including software and settings necessary for a typical IRS worker. - Second mode will demonstrate a slimmer software environment that provides secure access to a virtualization infrastructure. LPS provides a bootable CDROM and USB image for IRS, capable of booting various computers into a light client computing device suitable for accessing IRS data and services. Capabilities include remote access, a web browser for access to internal (IRS) web services, and a virtualization client for accessing Virtual Desktop Infrastructure (VDI) services.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
Yes Individual Taxpayer Identification Number (ITIN)
Yes Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes Practitioner Tax Identification Number (PTIN)

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

The system is the client environment that IRS workers interface with when running applications and accessing data; therefore, it is possible that any of this type of data could be displayed through the system, based on what the task of the IRS worker is and what they are accessing. The system does not inherently collect this data, but could display or store it based on the application the worker is using. For Windows ToGo, the mitigation strategy to protect SSNs that may traverse applications or services hosted by the client environment is the same as the IRS Windows 7 PC/Laptop systems (COE), including disk encryption, data encryption at rest and in transit, security software (firewall, virus/malware protection), and policies enforced to harden and lock the system down. These mitigations are implemented immediately (no forecast necessary). For LPS, mitigations include read-only environment to disallow storage of any data, protection from viruses and malware through firewall rules and read-only environment, and encryption of data in transit supporting enterprise remote access and access to encrypted web services.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
Yes	Place of Birth	No	No	No
Yes	SEID	No	No	No
Yes	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification	No	No	No

	Numbers (IP PIN)			
Yes	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
Yes	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
Yes	Photographic Identifiers	No	No	No
Yes	Biometric Identifiers	No	No	No
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	Yes

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
Yes	Proprietary data	Business information that does not belong to the IRS
Yes	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
Yes	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

The system provides the client environment to the user and does not inherently collect SBU/PII but can run applications or access services that may display SBU/PII. Business needs and uses of SBU/PII is determined and controlled by the applications and services that the user has accesses.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

The system provides the client environment to the user and does not inherently collect SBU/PII but can run applications or access services that may display SBU/PII. Accuracy, timeliness and completeness of SBU/PII is maintained by the applications and services that the user accesses.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Other

If **other,** explain your answer**.** The system is the client environment used to run other applications and does not inherently access SBU/PII. Access to SBU/PII would be controlled by other systems that are built for such access, but would operate on top of this client environment.

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Redacted Information For Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

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

14a. If **yes**, briefly explain how the system uses the referenced technology. Light Client is an example of Bring Your Own Device. Both the Windows To Go where the operating system, computing and storage are contained on a secured USB drive or Light Portal Solution where a Linux OS on a disc or USB device allow a secure connection to a virtual PC within the IRS network are examples of mobile technologies.

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No

17b. If **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.
Not applicable, there is no inherent data collection by the system.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? Not applicable, there is no inherent data collection by the system.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Not applicable, there is no inherent data collection by the system.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level(Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest.
Contractor Users	Yes	Read and Write	Low
Contractor Managers	Yes	Read and Write	Low
Contractor Sys. Admin.	No		
Contractor Developers	No		

21a. How is access to SBU/PII determined and by whom? The system provides the client environment to the user and does not inherently collect SBU/PII but can run applications or access services that may display SBU/PII. Access to SBU/PII is determined and controlled by the applications and services that the users authenticates to.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ? Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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? No

22b. 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.

All records housed in the Light Client Technology demonstration will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedules (RCS) 17 for Information Technology, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. The method used for sanitization will follow NIST SP 800-88 guidelines

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the systems audit trail. Application and data level logging is the responsibility of the application or service that accesses, modifies, and controls data. The client environments provided by Windows ToGo and LPS only provide the lower level operating environment and do not inherently access, modify, control or log data. As a for systemic logging, the Windows ToGo system provides the same event logging capability as general Windows based systems, including system, application, and security logging. Logs are stored on each instance of the device and accessible by administrators when necessary. The LPS technology is a read-only client environment that cannot store logs of local activities; however, accesses to data would be logged by the end system or service that is managing/controlling data.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. The light client solutions are in a technology demonstration phase which focuses on validation of functionality, capabilities and identification of use cases that might benefit from the technology. Testing during this phase is not intended to be of the comprehensive nature necessary for solutions that are approved for production use. If and when the technology proves valuable to the IRS and is approved as a production solution, a system test plan will be created and followed.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: Not Applicable
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report