Date of Approval: October1, 2018 PIA ID Number: **3705**

A. SYSTEM DESCRIPTION

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

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

ePostcard, PIAMS #1554

Enter the approval **date** of the most recent PCLIA. 11/06/2015

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of Personally Identifiable Information (PII)(PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
No Significant System Management Changes
No Significant Merging with Another System
No New Access by IRS employees or Members of the Public
No Addition of Commercial Data / Sources
No New Interagency Use
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

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

TE/GE Investment Executive Steering Committee

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

No Vision & Strategy/Milestone 0
No Project Initiation/Milestone 1
No Domain Architecture/Milestone 2
No Preliminary Design/Milestone 3
No Detailed Design/Milestone 4A
No System Development/Milestone 4B
Yes 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? Yes

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.
ePostcard is a web-based application used for online submission of Internal Revenue Service (IRS) form 990-N, Electronic Notice for Tax-Exempt Organizations, for annual filings for small tax-exempt organizations reporting $50,000 or less. ePostcard transmits submissions Modernized Electronic Filing (MeF). Pursuant to Internal Revenue Code (IRC) 6104, all information transmitted to IRS via IRS Form 990N is made publicly available via www.irs.gov approximately two weeks after submission.

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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

No	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
No	Legal/statutory basis (e.g. where collection is expressly required by statute)
No	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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

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

If **yes**, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
Yes	E-mail Address
No	Date of Birth

No	Place of Birth
Yes	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
Yes	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. 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
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
No	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.

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

If **yes**, describe the other types of SBU/PII that are applicable to this system.

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

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

If the answer to 6f is **No**, verify the authority is correct with the system owner and then update the answer to 6f.

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 IRS contractor, Accenture, pulls the National Accounts Profile (NAP) file from the IRS server. This file is pulled weekly to validate the users' need to access ePostcard. ePostcard is a web-based application that transfers submittals to the Modernized eFiling system (MeF). Once the users enter their information in the IRS Form 990N, it is transmitted to the IRS MeF production system. It must be noted that pursuant to IRC 6104, all information transmitted to IRS via IRS Form 990N is publicly available approximately two weeks after submission.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

The information is collected from the user and is displayed back to the user for verification prior to final submission. Field level and form level validation is used to ensure that inputs conform to the appropriate schema. Email addresses are verified by a process of sending a confirmation email to the provided address when the user obtains their login ID. The Form 990-N itself is final once submitted and cannot be modified directly on this system. The user/filer can log in and update their contact information at any time. ePostcard does NOT make determinations. All determinations are completed through the Examination and Rulings and Agreement process with no direct correlation to ePostCard.

C. 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.

9. 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

If **yes**, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
IRS 50.222	Tax Exempt/Government Entities (TE/GE) Case Management Records
IRS 34.037	Audit Trail and Security Records System

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

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

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
National Account Profile (NAP)	Yes	03/21/2017	Yes	08/04/2012

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

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms.

Form Number	Form Name
990-N	Electronic Notice (ePostard) for Tax Exempt Organizations Not Required to File Form 990

11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Modernized eFiling System (MeF)	Yes	02/23/2016	Yes	02/09/2018

Identify the authority. The Pension Protection Act of 2006 requires all tax-exempt organizations to file a return with the Internal Revenue Service (IRS) each year. This Act requires all small organizations to file electronically. MeF is the Service's avenue for all electronic filing.
For what purpose? The Pension Protection Act of 2006 requires all small organizations must file electronically. MeF is the Service's avenue for all electronic filing.

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? Yes
If **yes**, identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Accenture	electronic	Yes

Identify the authority ePostcard is a contractor owned and managed application. Accenture is the IRS contractor for ePostcard.

For what purpose? Accenture pulls the National Accounts Profile (NAP) file from the IRS server. This file is pulled weekly to validate the users' need to access ePostcard. ePostcard is a web-based application that transfers submittals to MeF. Once the users enter their information in the IRS Form 990N, it is transmitted to the IRS MeF production system.
Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?>
Yes

12.e. Does this system disseminate SBU/PII to other Sources? 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, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? Yes

16.a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16.a.1. If **yes**, when was the **e-RA** conducted? 05/14/2018

If **yes**, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

If **Level 2**, Confidence based on:

Single Factor Identity Validation

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
A Privacy Act Notice is present on the Form and displayed on the site prior to submission. Notice, consent and due process are provided pursuant to 5 USC.

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

18.b. If individuals do not have the opportunity to give consent, 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.

19. How does the system or business process ensure due process regarding information access, correction and redress?
A Privacy Act Notice is present on the Form and displayed on the site prior to submission. Notice, consent and due process are provided pursuant to 5 USC.

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)

Contractor 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	No	
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	High
Contractor Developers	Yes	Administrator	High

21.a. How is access to SBU/PII determined and by whom? A list of IRS users requiring access is provided to the contractor by IRS Electronic Products and Services Support (EPSS) e-helpdesk personnel. The contractor determines the administrators and developers requiring access based on the roles and requirements for system maintenance and provides the names and information to IRS program management for authorization. IRS EPSS e-helpdesk personnel must approve the contractor based on the following prior to granting access. 1. Assign software ID. 2. Conduct communication tests. 3. Review test submissions based on the test scenarios the Service provides. 4. Escalate for questions or final approval. 5. Once approved, the contractor is granted access. ePostcard is not an IRS managed application - it resides on and is managed by an IRS contractor. Therefore, OL5081 is 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? Yes

22.a. 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.

All records housed in the ePostcard system will be erased or purged from the system in accordance with approved retention periods for MeF. The method used for sanitization will follow NIST SP 800-88 guidelines. ePostcard is an input source to the MeF system, and as such will be managed according to requirements using IRS Records Control Schedules (RCS) 19, Item 81. Any new records or changes to the records retention requirements will be as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

I.2 SA&A OR ASCA

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

23.a. If **yes**, what date was it completed? 06/21/2018

23.1 Describe in detail the system's audit trail. The system logs events in keeping with the requirements of IRS Pub 4812 section 13.2. The logs are synchronized to a Security Information and Event Monitoring system for consolidation, alerting, and retention. The application logs include the following: • All login attempts (successful and unsuccessful) with records of timestamp, user ID, and IP address involved, as well as reason for failure. • All changes to user information (name, phone number, email address, password) are logged, including timestamp, old and new information (excluding password values), and user making the change. • All events affecting filing status of a form (starting a form, completing a form, filing a form) are logged, including timestamp, action taken, and user taking the action.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a If **yes**, If yes, was the test plan completed? Yes

24.a.1. If **yes**, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIT (Web-based document management system)

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? This effort is part of the Annual Security Control Assessment (ASCA) process.

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:

26.a. IRS Employees:	Under 50,000
26.b. Contractors:	Under 5,000
26.c. Members of the Public:	100,000 to 1,000,000
26.d. 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

27.a. If **yes**, explain the First Amendment information being collected and how it is used.

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission 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

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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