Date of Approval: December 3, 2018 PIA ID Number: **3796**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Field Assistance Scheduling Tool, FAST

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.

Field Assistance Scheduling Tool v2, FAST, O&M

Enter the approval **date** of the most recent PCLIA. 04/30/2018

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
Yes New Interagency Use
No Internal Flow or Collection
No 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.

Technology Integration Board (TIB)

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
No System Deployment/Milestone 5
Yes 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 Field Assistance Scheduling Tool (FAST) is an application to allow Field Assistance (FA) and Accounts Management (AM) employees to schedule appointments with taxpayers. The IRS employee (not the taxpayer) uses this system. FAST is a FedRAMP Moderate cloud-based solution leveraging a vendor product that includes a hierarchical set of user groups with varied access levels dependent upon the IRS employee's role. FAST will allow detailed metrics to be available for specific user groups to determine taxpayer trends and make strategic decisions based upon Taxpayer and Taxpayer Assistance Center (TAC) needs. Taxpayers call in to make an appointment, the AM assistor attempts to provide assistance over the phone. If they can't provide assistance, they access the FAST system to schedule an appointment. The tool allows the employee to specify whether the taxpayer needs an interpreter, Spanish speaking assistance, or other special needs, and will find them the closest TAC with those availabilities. An e-mail is auto-generated (containing no PII) to remind the taxpayer of the appointment time set. E-mail is sent according to Internal Revenue Manual (IRM) 10.5.1.6.8.1, Emails to Taxpayers and Representatives.

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:

Yes	Social Security Number (SSN)
No	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)
Yes	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.

SSN is needed. No plan to eliminate. The plan is to have the SSN put in the FAST scheduled appointment.

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

The Office of Management and Budget memorandum M-17-12 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. FAST requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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
No	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)
No	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
No	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.
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.
No	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.

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

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)
Yes	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

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.

PII is needed to capture taxpayer information: Name, phone number and email address to schedule face to face appointments in Field Assistance (FA) TAC. SSN will be needed in order to do an account review and any authentication needed before the taxpayer arrives for the appointment. Phone number is needed in case contact with the taxpayer is needed, and e-mail address will be used to generate an e-mail reminder of the appointment. No PII or SBU is included in the e-mail.

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

Taxpayer information is validated at the time of the scheduled appointment by FA employees. Taxpayers are taken through an approved authentication process before information is discussed.

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 00.009	Taxpayer Assistance Center Recorded Quality Review Records
IRS 34.037	Audit Trail and Security Records System
IRS 00.001	Correspondence Files and Correspondence Control Files

*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? No

F. DISSEMINATION OF PII

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, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

15. Does the system use cloud computing? Yes

15.a. If **yes**, Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified? Yes

If **yes**, Date Certified. 12/08/2017

15.b. Please identify the ownership of CSP data. IRS

Please identify the 3rd party.

15.c. Does the CSP allow auditing? Yes

Who audits the CSP data? 3rd Party

15.d. Please select background check level required for CSP. Moderate

15.e. Is there a breach/incident plan on file? Yes

15.f. Privacy laws (including access and ownership) can differ in other countries. If any data is considered SBU, will this cloud be Continental US (CONUS) only for:

Storage	Yes
Transmission	Yes
Maintenance (including backups)	Yes
Troubleshooting	Yes

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

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?
The Customer Service Representative will notify the taxpayer when requesting the SSN. Language will be used that has been approved by Counsel.

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

18.a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
Verbally to call site phone assistor.

19. How does the system or business process ensure due process regarding information access, correction and redress?
FAST is an appointment scheduling tool but due process is provided per Title 26 for any tax-related issues the taxpayer is inquiring about.

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 Contractor 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	Yes	Administrator

Contractor Employees? Yes

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

21.a. How is access to SBU/PII determined and by whom? The FA team has implemented a Role-based Access Control structure to access the data in FAST. The FA group has determined who gets access to the data. The user will be required to go through Online (OL) 5081 to request access to FAST. Access to the data is determined by the manager based upon a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the OL 5081 process to request access to the system.

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.

FAST recordkeeping data is approved for destruction in accordance with National Archives and Records Administration (NARA) Job Number N1-058-10-016. All records housed in the system will be erased or purged from the system after a three-year retention period as required under IRM 1.15.6 Managing Electronic Records. All records housed in the FAST system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has NARA approval to affect data disposition. Any records generated and maintained 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 Schedule 31,

Item 25b and as coordinated with the IRS Records and Information Management 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? 12/08/2017

23.1. Describe in detail the system's audit trail. All auditing for the FAST system will be handled by the contractor who uses a distributed deployment model to collect audit log data from servers and centralize indexing to support information searches and audits. Log data is captured locally on devices in syslogs. Login Events, Web Application Logs, System Events, User Account Management; Authorization Checks, Privileged Functions, System Events, Data Access, Data Changes, Data Deletions, Permission Changes, Object Access, and Policy Changes are the auditable events that will be captured by the system. FAST is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

J. PRIVACY TESTING

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

24.a. 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)? On the FAST Project SharePoint page.

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? Testing and validation activities will be conducted by the vender to meet FEDRAMP approved controls. Please note the application will inherit all vender FEDRAMP approved security controls.

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:	More than 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

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