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

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
Yes	Preliminary Design/Milestone 3
Yes	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 Field Assistance Scheduling Tool (FAST) is an application to allow Field Assistance employees and Accounts Management employees to schedule appointments with taxpayers. The IRS employee (not the taxpayer) uses this system. FAST is a FedRAMP Moderate cloud based solution leveraging ServiceNow that includes a hierarchical set of user groups with varied access levels dependent on 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 on Taxpayer and TAC needs. Taxpayers call in to make an appointment the accounts management 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 user (internal employees only) 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. No part of the system allows the taxpayer access to it.

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.)? No

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

No On Primary No On Spouse No On Dependent

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

- No Social Security Number (SSN)
- No Employer Identification Number (EIN)
- No Individual Taxpayer Identification Number (ITIN)
- No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
- No 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).

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
No	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
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
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.

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)
- 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

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 the criteria. Be specific. PII is needed to capture taxpayer information: Name, phone number and in the future email address to schedule face to face appointments in Field Assistance (FA), Taxpayer Assistance Centers.

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.

Taxpayer information is validated at the time of the scheduled appointment by FA employees.

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? Yes

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

<u>SORNS Number</u>	<u>SORNS Name</u>
Treas/IRS IRS 00.009	Taxpayer Assistance Center Recorded Quality Review
Treas /IRS 34.037	Audit Trail and Security Records System
Treas/IRS 00.001	Correspondence Files and Correspondence Control Fi

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

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

15. Does the system use cloud computing? Yes

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. Taxpayer information for scheduling appointments only.

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

18a. 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? Reduced Single Sign On access to 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 Contractor Operated

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

IRS Employees? Yes

<u>IRS Employees?</u>	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

<u>Contractor Employees?</u>	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

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

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? Yes

22a. 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 NARA Job Number N1-058-10-016. All records housed in the system will be erased or purged from the system after a 3-year retention period as required under Internal Revenue Manual (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 National Archives 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 ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? In-process

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 12/28/2017

23.1 Describe in detail the system's audit trail. All auditing for the FAST system will be handled by ServiceNow. ServiceNow uses a Splunk 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 and continuously sent to Splunk forwarders. 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

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 12/15/2017

24.3 If **completed/ or in process**, describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met? Testing and validation activities will be conducted by ServiceNow to meet FEDRAMP approved controls. Please note the application will inherit all ServiceNow 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:

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: More than 1,000,000
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
