NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: February 5, 2015 PIA ID Number: **1213**

1. What type of system is this? MARS - ETrak, MARS

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

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

Media Activity Recording System

Next, enter the **date** of the most recent PIA. 1/6/2012 12:00:00 AM

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

No	Addition of PII
Yes	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

Were there other system changes not listed above? No

If yes, explain what changes were made.

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
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.

There are four primary uses for the MARS program. First, media specialists can use the program as a resource for searching their own activity and that of their peers to determine if there have been prior inquiries on a certain or similar topic. This research can then lead them to an approved response, an SME or a peer who can help explain the nuances of a particular issue. Second, managers can use the report to track the overall and detailed activity of individual specialists or their own work group. Third, management can use the information to inform internal BOD stakeholders and oversight groups such as TIGTA or GAO with respect to media activity and thus media relation support for specific campaigns, events or topics. Fourth and finally, the data is used to provide input for the Media relations portion of the C&L Division Business Performance Review (BPR).

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, 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 variations of SSN s (i.e. last 4 digits, etc.)? No

If **yes**, check who the SSN (or SSN variation) is collected on.

No On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) 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	Preparer Taxpayer Identification Number (PTIN)

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

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

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	No	No	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
No	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
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that 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 Letter of Understanding (LOU)	Documents that have been marked OUO or LOU
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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The MARS system records the media contact activity of media relations specialists. PII can be recorded but is not required. PII relating to the public generally includes: News Media Outlet Name, Address, Telephone Number, Email Address, Reporter/Editor/Journalist Name and News Media Type (newspaper, radio, TV, web site, etc.) Also, included is a reference to the IRS media specialist's name and possibly the name and telephone number of other IRS employees who might be SMEs. There is no specific return information. Employees that create MARS records do not have access to tax returns or to IRS systems that record private taxpayer account information.

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.

PII can be recorded but is not required. PII relating to the public generally includes: News Media Outlet Name, Address, Telephone Number, Email Address, Reporter/Editor/Journalist Name and News Media Type (newspaper, radio, TV, web site, etc.) Also, included is a reference to the IRS media specialist's name and possibly the name and telephone number of other IRS employees who might be SMEs. There is no specific return information. Employees that create MARS records do not have access to tax returns or to IRS systems that record private taxpayer account information.

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.

SORNS Number	SORNS Name
Treas/IRS 36.003	General Personnel and Payroll Records
Treas/IRS 10.004	Stakeholder Relationship Management and Subject Fi
Treas/IRS 34.037	Audit Trail and Security Records System

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

N/A

E. INCOMING PII INTERFACES

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

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

No System Records found.

11b. Does the system receive SBU/PII from other federal agency or agencies?

No Organization Records found.

11c. Does the system receive SBU/PII from State or local agency (-ies)?

No Organization Records found.

11d. Does the system receive SBU/PII from other sources?

No Organization Records found.

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

No Tax Form Records found.

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)?

No Employee Form Records found.

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

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

No System Records found.

12b. Does this system disseminate SBU/PII to other Federal agencies?

No Organization Records found.

12c. Does this system disseminate SBU/PII to State and local agencies?

No Organization Records found.

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors?

No Organization Records found.

12e. Does this system disseminate SBU/PII to other Sources?

No Organization Records found.

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.? No

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

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.
Senior Management in Media Relations has determined that managers and employees who are directly responsible for media contact should have access to the system. Therefore those managers and employees, each of who are likely to have a need to create a record of media contact must by definition have read and write access. The system administrator and developers require access to the system to debug software or operational glitches. As a general rule other communications and non-communications employees do not require and are not granted access. If a unique need arises for access then Senior Management and Executive leadership within the Office of Communication would make the decision to grant read only access for a limited use purpose.

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

If no, why not? Senior Management in Media Relations has determined that managers and employees who are directly responsible for media contact should have access to the system. Therefore those managers and employees, each of who are likely to have a need to create a record of media contact must by definition have read and write access. The system administrator and developers require access to the system to debug software or operational glitches. As a general rule other communications and non-communications employees do not

require and are not granted access. If a unique need arises for access then Senior Management and Executive leadership within the Office of Communication would make the decision to grant read only access for a limited use purpose.

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

The basic data regarding what media outlet and who within the media outlets is seeking information is required to maintain a record of media inquiries and the information provided to them. We need to know the names, addresses, telephone numbers and email address in order to respond to the inquiries and then we need retain that information for an historical record of who asked what questions. We need to keep track of which IRS employee responded to the media inquiry this we need to capture the employee's name and contact information as well as capturing how the IRS spokesperson (media relations specialist) responded. In addition we periodically need to seek advice and input from a Subject matter Expert (SME) in which case we also need to record who provided the specific expertise. This information is needed on occasion to inform senior leadership regarding an issue that has received attention in the media. This information is sometimes used to brief program managers or even to prepare for congressional inquiries. The information is also used by other media specialists to compare and contrast inquiries and response on the same or similar tax topics for consistency. Underlying all of this is the objective of education the public and increasing public awareness of tax law and procedures that affect their filing and payment of federal taxes.

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	Read-Only
Developers	Yes	Administrator

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Senior Management in Media Relations has determined that managers and employees who are directly responsible for media contact should have access to the system. Therefore those managers and employees, each of who are likely to have a need to create a record of media contact must by definition have read and write access. The system administrator and developers require access to the system to debug software or operational glitches. As a general rule other communications and non-communications employees do not require and are not granted access. If a unique need arises for access then Senior Management and Executive leadership within the Office of Communication would make the decision to grant read only access for a limited use purpose.

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

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.

MARS is unscheduled. A request for records disposition authority for MARS data and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for MARS inputs, system data, outputs, and system documentation will be published in Records Control Schedule (RCS) Document 12990 under RCS 34 for Communications, Item 12.

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)? Yes

23a. If **yes**, what date was it completed? 1/6/2012 12:00:00 AM

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

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

23.1 Describe in detail the system s audit trail. The modernized system will track employee access through system activity log. All data entries are saved into an electronic database. The database is routinely backed up to maintain an audit trail of records as the exist when they are entered and as they are changed.

I.2 SA&A OR ECM-R

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

If **yes**, Is the test plan in process or completed: Completed

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?

The eTrak system is maintained by the IRS and has been approved and tested. When a member of the media contacts the IRS, the individual is asked the following: What company do your represent, what is your own name and position, what is your mailing address, telephone number

and email address. Whatever information is provided will then be recorded. In the event that the contact is initiated by the IRS media relations specialist then that specialist has already obtained much of this information based on existing public records.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? The eTrak system is maintained by the IRS and has been approved and tested.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live 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: Not Applicable
26c. Members of the Public: Not Applicable
26d. Other No

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

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? Yes

If **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. No fields have been included that capture SSN, EIN or other TIN information. Specialists will be given instructions to not include such information in the Comments Narrative field. This system allows employees to look up past official interactions with the press and media.

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees or IRS contractors 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