A. SYSTEM DESCRIPTION

1.   Enter the full name and acronym for the system, project, application and/or database. Enforcement Revenue Information System, ERIS

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, PIA ID Number and milestone of the most recent PIA.

>>   Enforcement Revenue Information System, ERIS, Maintenance 1164

>>   Next, enter the **date** of the most recent PIA.   1/29/2015

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

No	Addition of PII
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

>>   Were there other system changes not listed above?   No

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
Yes	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.

Enforcement Revenue Information System (ERIS) is a cross-functional data repository consisting of raw data warehouse and summary database that tracks the amount and timing of revenue from all IRS enforcement functions, along with the direct hours spent on the cases, where available. It is the only system that tracks enforcement cases across functions, and that captures the dollars actually collected on these cases. The IRS Commissioner and other IRS executives require the support of this automated system, which is designed primarily to enable them to more accurately measure the results of the IRS enforcement activities and to assist them in performing forecasts of direct hours and revenue. IRS managers also require the system to provide information that will aid them in managing enforcement functions, obtaining accurate measures of direct hours and revenues, and obtaining comprehensive information on direct hours and yields. The Commissioner, executives, and managers can use ERIS information to improve the accuracy of functional planning models and to direct their attention to areas where concentrated efforts will be most effective. For example, if executives can obtain specific, current information, they can then consider new approaches to workload management and enforcement function planning from both high-level and detailed perspectives.

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   No   On Spouse   No   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)
   No   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).

   End users access ERIS data on Compliance Data Warehouse (CDW) where SSN/EIN/TIN are masked. Real TINs are used only for ERIS processing as SSN/EIN are the only way to match data to specific taxpayer accounts. Besides SSN/EIN/TIN no other PII is used for ERIS. The Office of Management and Budget memorandum M-07-12 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. The Enforcement Revenue Information System (ERIS) requires the use of SSN's 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.

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
No	Name	No	No	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	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
Yes	Tax Account Information	Yes	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

elected	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.
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
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

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 this criteria. Be specific.

ERIS is the only application that tracks an enforcement case from start to finish, incorporating information from all of the various enforcement functions where the case was worked. ERIS delivers data, provides tools, and computing services to the Research Community to support projects, data analysis, prediction, simulation, and optimization studies. ERIS matches taxpayer-level data from different data sources by using TIN/SSN/EIN. ERIS has to account for specific taxpayer enforcement interactions/transactions and the only way to allocate this information to a specific taxpayer is through the unique identified - TIN/SSN/EIN.

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

Accuracy/Completeness - ERIS receives data from trusted internal sources. The data received by ERIS is verified by the various applications as being complete and accurate prior to being transmitted to ERIS. Additionally, ERIS schema is configured in accordance with its data sources; thus, the data, when it is retrieved via batch processing, will automatically load in the right format. One of ERIS's objectives is to provide reports that directly reflect the information provided by the various divisions with little or no modification. Timeliness – Data is received on regularly batch processes schedule (either weekly or monthly depending on the systems providing the data to ERIS). The schedule is base in accordance with established agreements between the ERIS project office and the project offices of the individual suppliers.

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 24.030	Customer Account Data Engine (CADE) Individual Master File
Treas/IRS 24.046	Customer Account Data Engine (CADE) Business Master File
Treas/IRS 34.037	Audit Trail and Security Records System
Treas/IRS 26.019	Taxpayer Delinquent Accounts Files

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?   Yes

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

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

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Individual Master File - IMF	Yes	05/02/2014	Yes	11/15/2012
Business Master File - BMF	Yes	06/02/2014	Yes	05/23/2013
Automated Non-Master File - ANMF	Yes	07/22/2014	Yes	10/17/2012
Audit Information Management System - AIMS	Yes	08/21/2012	Yes	10/16/2014
Examination Return Control System - ERCS	Yes	01/29/2014	Yes	04/10/2014
Tax Preparer PTIN System - TPPS	Yes	01/08/2013	Yes	08/13/2014
Integrated Collection System - ICS	Yes	09/19/2013	Yes	04/10/2014
Information Returns Processing Case Analysis - IRPCA	Yes	03/12/2014	No	04/10/2014

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

11c. Does the system receive SBU/PII from State or local agency (-ies)?   No

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

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

    14a. If **yes**, briefly explain how the system uses the referenced technology.

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.
    The Enforcement Revenue Information System (ERIS) is not a system that directly collects information from taxpayers. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. ERIS uses information from other IRS systems to give a full accounting of what transpired on an enforcement case.

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?   The Enforcement Revenue Information System (ERIS) is not a system that directly collects information from taxpayers. ERIS uses information from other IRS systems to give a full accounting of what transpired on an enforcement case. ERIS does not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent and due process are provided in the tax forms instructions filed by the taxpayer, and pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
    The Enforcement Revenue Information System (ERIS) is not a system that directly collects information from taxpayers. ERIS uses information from other IRS systems which provides the due process to give a full accounting of what transpired on an enforcement case.

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-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	No	

    Contractor Employees?   Yes

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

    21a. How is access to SBU/PII determined and by whom? Requests for access to the Enforcement Revenue Information System (ERIS) by IRS personnel are made through the On-Line 5081 (OL 5081) process and must be approved by the requestor's manager and/or security representative. External requestors (such as contractors, Treasury, Government Accountability Office (GAO) et al) must use the paper Form 5081, and obtain approvals from the Contractor Technical Representative (COTR), security representative, ERIS Project Manager. Approval and authorization are granted based on signatory acknowledgement and agreement to comply with the Rules of Behaviors, complete security-related training. The level of data access is limited to that which is specified in the approved proposal request and those established through assigned rights and privileges.

    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.

ERIS data is approved for destruction 20 years after case is closed, or when no longer needed for operational purposes, whichever is later (Job No. N1-58-10-5, approved by the National Archives and Records Administration 12/21/2010). Data retention requirements, along with disposition instructions for ERIS inputs, outputs and data documentation will be published under IRM 1.15.27 Records Control Schedule for Compliance Research, item 55 when next updated. One-year's worth of ERIS data is maintained at any one time as a back-up for disaster recover/data validation purposes. Deletion of this reference material occurs monthly on a rolling basis, one-year from its creation data. Every data file placed on ERIS is time/date stamped. After loading data from tapes, they are degaussed at ECC-MTB. Paper data is shredded.

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?   7/17/2014

        23.1 Describe in detail the system s audit trail. ERIS relies on the Resources Access Control Facility (RACF) auditing capabilities at the mainframe system log. At a minimum, an event record shall specify the following: • Logon and logoff information • Password changes • All systems administrator (SA) actions while logged on to the system as an SA and as a user • Files accessed, modified and deleted.

J. PRIVACY TESTING

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

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

        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?
1. Accountability: Applications that generate data for end users that contains PII have been modified to include privacy warnings. PII-specific data is transmitted to end users via encrypted protocols. 2.- Purpose Limitation: ERIS access is governed by OL5081 and only users with a business need are granted access. Annual recertification ensures access is reviewed. 3.- Minimization of Collection, Use, Retention, and Disclosure: In addition to IRS policy regarding least required privileges and access, only users with a business need are granted access via OL5081. In addition to IRS access restriction policies, contracting vehicles and policies require the narrowest degree of data collection necessary to fulfill ERIS' mission and minimize programming services required to be purchased by the government. 5.- Strict Confidentiality: ERIS access is governed by OL5081 and only users with a business need are granted access. Annual recertification ensures access is reviewed. 6.- Security: ERIS is a FISMA reportable system and undergoes annual testing for security certification. 10- Privacy Awareness and Training: All employees and contractors must complete security and privacy training annually and certification is tracked by IRS Management.

        24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?   ERIS Test Plan and Test Results are stored on SharePoint: https://organization.ds.irsnet.gov/sites/ras/ERIS/DRC%20Deliverables%20Ph%2019/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fras%2FERIS%2FDRC%20Deliverables%20Ph%2019%2FD

RC%20Deliverables%20Ph%2022%2FIV%20and%20V%20%2D%20Test%20Plan%20and%20Test%20Results

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. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing?   Yes
    25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?   Yes

    If **yes,** provide the date the permission was granted.   8/14/2014

    25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments?   Yes
    .

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: 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? 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. ERIS is used to perform research studies that may identify an individual taxpayer or group of taxpayers. When used to identify individual taxpayers by TIN the requestor must submit a valid request with an approved business purpose with authorization to view sensitive but unclassified (SBU) data. This information can be requested to evaluate the impact of program or policy changes on specific groups of taxpayers, and develop workload models to optimize the use of resources. These aggregate groups could be identified as non-filers, by balance due amounts.

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? <u>No</u>

<u>End of Report</u>