Date of Approval: February 5, 2018 PIA ID Number: **2932**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. IRS Video Portal File Management System, IVPFMS

2. Is this a new system? Yes

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

Yes	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.

The IRS Video Portal (IVP) website distributes video and audio content to the public and to IRS employees. IVP presentations are designed to enhance the public's understanding of the IRS and its mission, programs and policies. The IVP also provides information and training to IRS employees. The IVP File Management System (IVPFMS) currently enables authorized IRS personnel to upload media and other files required for IVP presentations. Producers and editors, both inside and outside of the IRS, of multi-media presentations require the ability to transfer media files between the IRS and external systems. This proposed change to the IVPFMS is the addition of a membership system to identify IRS users and to authenticate and identify non-IRS (external) users. The IVPFMS membership system will store name, email address and the Standard Employee Identifier (SEID) for each IRS user. A recently issued federal mandate, BOD 18-01, requires that all public-facing federal websites use the secure HTTPS web protocol. Storing name, email and SEID on IVPFMS is required because IRS internal servers run HTTP (a non-secure protocol) instead of HTTPS. To identify IRS users on administrative pages and on reports, the IVPFMS can no longer fetch name, email and SEID from IRS servers because this mixes non-secure with secure content on IVPFMS web pages defeating the purpose of moving to HTTPS. Non-IRS users will be registered with a name, email address and password. When the appropriate IRS authorities grant permissions for that email address, the user will be able to download or upload files via the IVPFMS. The uploaded files will be automatically scanned for viruses and malware before being made available for distribution. IVPFMS membership will enable the IRS to reduce use of removable (DVD and flash drive) media and the time required to walk, drive or otherwise deliver the physical media. It will reduce the need to move media using external systems over which the IRS has no control. Benefits of adding membership for external users to the IVPFMS include: 1. Files will be unambiguously associated with pre-approved projects. The need to select a project before uploading or downloading media will prevent using a file with the wrong project. 2. There will be a complete record of file history including exactly when a file was uploaded

or downloaded and by which individual (as identified by email address.) Reporting which includes the names and email addresses will be restricted to specific IRS internal users who will be responsible for ensuring that the addresses are not disclosed. 3. The system will be able to "Unpublish" material which is out of date. 4. Non-IRS users will be registering directly on an IRS system. This removes the necessity of asking them to share their email addresses with a third-party identity system to interact with the IRS.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
No	Mailing address	No	No	No
No	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? No

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 this criteria. Be specific.

The only PII used in this system is the user's name and email address. For IRS users, SEID is also used. The email address is required to provide a unique User Name for authorized users of the

system. The email address will be voluntarily submitted by a registering user. When the new user's account is enabled, the email address will serve as the User Name for logging in to the system. In addition, if the user forgets her/his password, a message will be sent to the user at email address. The message will contain a one-time-use hyperlink to reset the password. The user's first name and last name will be used on reports which show usage of the system. These reports are available only to authorized IRS staff and to system administrators.

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

The end user is responsible for submitting a valid email address. A registration confirmation message sent to the email address will contain a hyperlink to confirm to the system that the address is valid. The user will need to click on the hyperlink in registration confirmation message for the system to enable the account. The page which allows the user to enable the account contains a message explaining that by enabling the account, the user understands and agrees to use of their name and email address. A user will be able to remove the account (and thus delete the email address and password from the system) at any time.

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
10.004	Stakeholder relationship management

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? 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? Yes

17a. 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?
Access to the registration system is by invitation only. The email address, first name and last name of a prospective user are registered in the system to create a tentative account. An email message providing a link which the prospective user can use to activate the account by entering and confirming a password. If the prospective user does not activate the account within a short period of time, the tentative account is removed from the system. A notice on the activation page describes the purposes for which the email address, first name and last name will be used.

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):
A user can decline to activate an account. A user indicates consent by clicking on the activation link in the invitation email and entering a password.

19. How does the system or business process ensure due process regarding information access, correction and redress?
This does not apply to the use of name and email address in this 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

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	No	
Developers	No	

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? The system provides reports of activity. Activity consists of records of files uploaded or downloaded. The reports associate the email address, first name and last name with each upload or download transaction. These reports are accessible only to IRS personnel granted explicit privileges to read them and to system administrators and software developers. The system administrator grants report access to an individual only with explicit written approval from the IRS manager in charge of 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.

All records housed in the IVPFMS system will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents, but contains a user portal to access video that has National Archives approval affecting data disposition. The IRS records accesses through the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be maintained using IRS Records Control Schedule (RCS) 34 for Communications and Learning, Item 7, and as coordinated with the IRS Records and Information Management (RIM) 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)? No

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

23.1 Describe in detail the system s audit trail. Only authorized and authenticated administrators will be able to change edit membership records. Each of these changes will be logged with the date and time of the change and the identity of the administrator making the change. When an end user makes a password change, this event will be logged as well although the password itself will not be human readable. An audit report utility will provide lists of all changes to the membership data.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. The collection and use of the email address is implemented using the functionality built into the Microsoft .NET development. IVPFMS adds first name and last name and, for IRS users, an SEID to the Microsoft .NET Identity system which controls security and which already contains the email address.

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: Not Applicable
26b. Contractors: Under 5,000
26c. Members of the Public: Not Applicable
26d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).
External multi-media editors' names and email addresses. This will be less than 10,000 records.

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