Date of Approval: June 16, 2017 PIA ID Number: **2604**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Web Content Management System, WCMS

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
Yes	Project Initiation/Milestone 1
Yes	Domain Architecture/Milestone 2
Yes	Preliminary Design/Milestone 3
Yes	Detailed Design/Milestone 4A
Yes	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? 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.

The Internal Revenue Service (IRS) decided to replace the current OpenText Web Content Management System (WCMS) for IRS.gov, EITC.IRS.gov, MARKETINGEXPRESS.IRS.gov and STAYEXEMPT.IRS.gov websites with the Drupal 8 WCMS. The IRS intends to leverage industry leading practices and innovations to improve the aforementioned websites' efficiency, effectiveness, quality, and process maturity while satisfying growing demands for secure, reliable, timely, and customer-centric Web solutions. The new WCMS is only available to authorized system users. Taxpayers do not access the WCMS system itself. Taxpayers consume the content which is published by the system and cached in the Akamai content delivery network. The IRS mission is to provide America's taxpayers top-quality services by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all. The IRS.gov website is the Agency's gateway to online self-service options for taxpayers, tax professionals and other customers. The overall effectiveness of IRS's digital service offerings depends on the quality, organization, and presentation of Web content on IRS.gov. By moving the current IRS.gov Web content management to a Drupal WCMS, the IRS expects to achieve more flexibility in managing the functionality of Web content management and presentation, allowing the Agency to optimize website customer experience across a variety of modern digital devices, including mobile. Drupal is a popular open source WCMS that has been widely accepted and used by many agencies within the federal government. IRS expects the Drupal WCMS solution to provide the flexibility and autonomy for IRS to incorporate new capabilities, templates, and features on a regular basis. The Drupal WCMS is hosted in Acquia. Acquia is a FedRAMP certified cloud service provider. Acquia's FedRAMP documentation is reviewed by IRS Cyber Security as a part of the Security Change Request process. Additionally, Cyber will be conducting an Event Driven Security Controls Assessment on the Drupal WCMS component. Acquia's FedRAMP documentation can either be retrieved from IRS Cyber Security or someone may request access to their FedRAMP package via

the official FedRAMP access request form. Proposed functionality: Replace current Google Search Appliance with data stored in Drupal WCMS and organized by Acquia Search. The approach will allow the IRS to manage the efile provider information currently displayed on the IRS.gov website using the Drupal WCMS, similar to how they manage other website content. The content managed within the Drupal WCMS will be made available to the taxpayer through the website, cached by the Akamai content delivery network. The taxpayers will not directly access the Drupal WCMS. Similar to content, they will consume the information which is published and made available by the system. The data which will be consumed includes business contact information (name of business, business address, point of contact and telephone number) for those who have become authorized efile providers and have given the IRS permission the IRS to post their contact information. Providers have the ability to "opt out" if they do not want their information posted to the IRS.gov website. All of this information is currently displayed in publicly accessible pages on IRS.gov today. This update is a change to where the content is managed, moving to the Drupal WCMS and Acquia Search.

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.

On Primary	On Spouse	On Dependent	Selected	PII Element
Yes	Name	Yes	No	No
Yes	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? 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.

IRS email addresses, names, and SEIDs will be passed to the Drupal system by the IRS Active Directory Federation Services to authenticate IRS users to the Drupal system via single sign on. No data will be passed back to the IRS ADFS system. E-Mail address is required to meet requirements regarding notifications for content updates with name and SEID needed for authentication and auditing. The eFile provider search returns business contact information (name of business, business address, point of contact and telephone number) for those who have become authorized efile providers and allows the IRS to post their contact 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

The scope of the SBU/PII data collected pertains only to IRS system user accounts and eFile provider business contact information. The user account information is ingested from IRS ADFS. The IRS ADFS system manages the information and sends it over to the WCMS system. The WCMS system does not collect SBU/PII for taxpayers. The efile provider business contact information is provided by the IRS via a data file SFTP'd to the IEP - PUP environment for loading. Today, the file data is loaded into the Google Search Appliance and going forward, the file data will be loaded into the Drupal system.

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
IRS 34.037	Audit Trail and Security Records System
IRS 36.003	General Personnel and Payroll Records

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 PCLIA	Approval Date	SA&A?	Authorization Date
IRS Active Directory Federation Services (ADFS)	Yes	07/02/2014	Yes	02/09/2017

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 agencies? 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.? Yes

14a. If **yes**, briefly explain how the system uses the referenced technology. The WCMS application is running on the Acquia FedRAMP Moderate Platform as a Service (PaaS). The Acquia PaaS is supported by the AWS US East & West Infrastructure as a Service (IAAS)/

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? 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?
A warning banner is defined and displayed per IRM requirements and displayed to the system user before access to the system. There is no public access to the WCMS system. No taxpayer will access the WCMS.

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):
The warning banner will remain on the screen until the system user acknowledges the usage conditions and takes explicit action to log onto the system. There is no public access to the WCMS system. No taxpayer will access the WCMS.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The warning banner will remain on the screen until the system user acknowledges the usage conditions and takes explicit action to log onto the system. There is no public access to the WCMS system. No taxpayer will access the WCMS.

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)

Contractor 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	Administrator
Developers	Yes	Read and Write

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	Read and Write	Moderate

21a. How is access to SBU/PII determined and by whom? WCMS implements a Role-based Access Control structure (RBAC) to access this data. A potential user will request access via the OL5081 system. This request has to be approved by the potential user's manager based on a user's position and need-to-know.

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.

WCMS recordkeeping data is approved for destruction in accordance with NARA Job No. N1-58-06-1, as approved July 3, 2006. Final disposition instructions for web content records, as well as management and operations records, are published under RCS 17 (Records Control Schedule for Information Technology), Document 12990, Item 25. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6 Managing Electronic Records. Audit logs, however, are maintained in accordance with General Records Schedule (GRS) 3.1, Item 020 (published in IRS Document 12829) and will be deleted/destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. Further guidance for the capture and retention of audit-related records is found in IRM 1.15 and IRM 10.8.3 Audit Logging Security Standards, section 10.8.3.2.2.

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. In compliance with the IRM 10.8.3, Event Content Requirement, the following data elements and fields are collected for Operating System and Network Content of Audit Records: The WCMS leverages the IEP Audit Plan. Based on the IRM, risk assessment and mission/business needs, Accenture has defined the following auditable events for WCMS: 1 Log onto system 2 Log off of system 3 Change of Password 4 All system administrator (SA) commands, while logged on as an SA 5 Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS) 6 Creation or modification of superuser groups 7 Sub-set of security administrator commands, while logged on in the security administrator role 8 Sub-set of system administrator commands, while logged on in the user role 9 Clearing of the audit log file 10 Startup and shut down of audit functions 11 Use of identification and authentication mechanisms (e.g., user id and password) 12 Change of file or user permissions or privileges (use of suid/guid, chown, su, etc.) 13 Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system. 14 Changes made to an application or database by a batch file.

15 Application critical record changes 16 Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility) 17 All system and data interactions concerning Taxpayer Data 18 Successful and unsuccessful account logon events 19 Account management events 20 Object access 21 Privilege functions 22 All administrator activity 23 authentication checks 24 authorization checks 25 Data deletions 26 Data access 27 Data change 28 Permission changes

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? 05/15/2017

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 are primarily conducted during through the Annual Security Controls Assessment (ASCA), which tests security and privacy 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: Not Applicable
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? Yes

If **yes**, does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Not Applicable

30b. If **N/A**, explain the Exemption and/or Disclosure s response. The WCMS does not process returns nor do the contractors or IRS employees in PPMO have access to returns.

End of Report