U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: DOI.GOV Website/DOI Drupal Content Management System (CMS)
Bureau/Office: Office of Communications
Date: September 30, 2021
Point of Contact
Name: Teri Barnett
Title: Departmental Privacy Officer
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Department of the Interior (DOI) Office of Communications manages the DOI Drupal Content Management System (CMS) Platform-as-a-Service (PaaS), which is an Open Source Software tool for creating, and managing content on websites. DOI uses Drupal CMS to publish

and manage content on the DOI.gov website to provide information on the Department's mission, vision, history, the nation's natural resources, cultural heritage, and to also engage with the public.

DOI Drupal CMS offers features such as a responsive web design to enhance user engagement across multiple devices, multilingual support for translating content, or for building audience-specific content, customizable workflow for content administration to meet publishing standards, customizable security compliance with standards such as Federal Information Security and Modernization Act (FISMA), built-in accessibility with Section 508 of the Rehabilitation Act of 1973 and Web Content Accessibility Guidelines (WCAG) 2.0 standards compliance, and key functions like custom promotions, drag-and drop layout, custom web forms, press releases, blogs and directories.

DOI Drupal CMS provides a fully functional hosted content architecture and capacity to host sub-pages of DOI bureaus and offices per separate individual procurement arrangement. Drupal CMS permits authorized DOI staff to electronically administer the content of DOI sites and explicitly maintain the functional independence of content management on individual sites. Each DOI bureau/office is under a separate acquisition plan for its use of DOI Drupal CMS platform and is responsible for their website content development and management activities in addition to complying with DOI Privacy Policy, Federal laws and policies to protect individual privacy.

Each DOI bureau/office data owner is responsible for ensuring their use of DOI.gov and DOI Drupal CMS follows applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. DOI.gov has a variety of forms and other documents supporting bureau and office programs and activities. Data owners are responsible for working with their bureau/office Associate Privacy Officer (APO) to identify, assess, and manage privacy risks related to their use of Cloud Drupal CMS system and DOI.gov, including conducting privacy impact assessments (PIAs) and providing privacy notice as appropriate and required. This PIA covers DOI.gov on Cloud Drupal CMS.

Visitors to the DOI.gov website have the option to enter their email addresses for GovDelivery to subscribe to the website's email notifications on topics they are interested in, which allows them to subscribe quickly and easily based on their individual needs and interests. DOI conducted a separate PIA to evaluate the use of GovDelivery. Please see the GovDelivery PIA for an assessment of the privacy risks.

C. What is the legal authority?

43 U.S.C. 1451, Establishment; Presidential Memorandum to the Heads of Executive Departments and Agencies on Transparency and Open Government, January 21, 2009; OMB M-10-06, Open Government Directive, December 8, 2009; OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, June 25, 2010; OMB M-10-23,

Guidance for Agency Use of Third-Party Web sites and Applications, June 25, 2010; OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☒ Other: *Describe*

This privacy impact assessment covers both DOI.gov website and Drupal CMS.

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code*

The UII code for Drupal CMS is 010-000002073. The UII code for DOI.gov is not available.

Drupal CMS System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

Drupal does not require a SORN. However, there are numerous program subpages within DOI.gov that may collect, maintain or process PII through webforms, blog comments, emails, or any other form of feedback, which are managed by a bureau/office data owner or a program

official, that may create records that are covered under existing Department-wide, bureau/office, or government-wide SORNs. The data owners and program officials are responsible for meeting the requirements of the Privacy Act for any collection, maintenance, use and sharing of records subject to the Act, including publishing SORNs and addressing complaints or requests for notification, access or amendment under the Privacy Act.

H. Does this information system or electronic collection require an OMB Control Number?

☐ Yes: *Describe*
☒ No

Bureaus and offices using web forms to collect information from members of the public are responsible for contacting their Information Collection Clearance Officer to address specific requirements under the Paperwork Reduction Act and obtaining the OMB Control Numbers as necessary and applicable.

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Personal Cell Telephone Number
☒ Personal Email Address
☒ Home Telephone Number
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

The system is single sign on being authenticated with the user's PIV Card. Each bureau manages their own users.

Individuals are not required to provide PII to use the DOI.gov website. Website visitors may elect to provide their name or contact information when they contact DOI officials through various web forms, use the "Contact Us" feature to provide comments or feedback, or send an email to program webpage points of contact. Information generally includes name and email address and may sometimes include address and phone number that is provided by the user when communicating with DOI. This "Contact Us" feature allows visitors to ask questions, make comments, or request information or services and helps DOI program officials engage the public, provide customer service and respond to visitor requests.

The DOI privacy policy is available on DOI.gov and describes the DOI privacy practices and the information collected by the DOI.gov website. The default web log information collected and stored by DOI.gov includes: internet domain, Internet Protocol address, browser type, operating

system, date and time, session cookies, pages visited on DOI website and search terms used from an external agency to get to DOI.gov. This default information is collected to enhance user experience and allow an electronic device to remember specific information about the user's session while on the DOI website to improve the experience. DOI.gov does not use persistent cookies that collect PII, as outlined in OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*.

Visitors to DOI.gov and members of the public interested in receiving updates on the Department's activities via email are redirected to GovDelivery to voluntarily subscribe for email notifications based on their interests. There is also an option to include password protection to subscriber preferences. Contact information provided will be used to deliver requested updates or to access subscriber preferences such as news, social media, and What we do. DOI conducted a separate PIA for use of GovDelivery, which may be viewed at https://www.doi.gov/privacy/pia.

Drupal CMS is independently used by bureau/office data owners to collect and manage bureau/office websites. This collection by bureau/office data owners may include a wide range of PII types including but not limited to: names, email addresses, telephone numbers, Social Security numbers (SSNs), dates of birth, financial information, employment history, educational background, correspondence or comments from members of the public, and other information related to a specific mission purpose. Each bureau/office data owner is responsible for ensuring that a Privacy Act statement or Privacy Notice specific to their program is available at the point of collection for their website to inform the public on how their information will be used, and must provide a link to the DOI Privacy Policy on all their webpages. Data Owners are responsible for working with their bureau/office APOs to identify, assess, and manage privacy risks related to their use of DOI.gov or the Cloud Drupal CMS system to collect, use, or disseminate PII, to ensure any risks have been properly assessed and addressed as necessary, in alignment with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Website
☐ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*

Access to Drupal CMS is limited to authorized DOI personnel and is controlled through user account management and authentication with the DOI Active Directory system and DOI's centralized user account management process.

☐ Other: *Describe*

D. What is the intended use of the PII collected?

PII collected from individuals who visit DOI.gov is used to respond to their comments, questions, requests for information or services, and to optimize the user experience while on the website. DOI.gov has a wide range of published content to engage the American public in the Department's missions and activities, to promote transparency and collaboration. In support of unique bureau/office programs and initiatives, published data by bureau/office data owners are used to provide awareness on new and existing programs across a broad range of the Department's operations. Forms or surveys may be used on DOI.gov that are specific to a program office and are evaluated in other privacy impact assessments. Each bureau/office data owner is responsible for ensuring that data published on their website using Drupal CMS is for authorized purposes, and any form, survey or collection or use of PII is described in the Privacy Act Statements and/or Privacy Notices provided to the individual at the point of collection in accordance with Federal laws, directives and DOI policy to protect individual privacy.

For Drupal, limited PII of authorized DOI employees and contractors is used to establish and manage user accounts in order to access and use the Drupal CMS tool to manage and publish content for the DOI.gov website.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

The purpose of DOI.gov is to disseminate information and engage the public. PII may be shared internally to facilitate that engagement or to communicate and respond to requests from members of the public. Limited PII is shared within the Office of Communications to grant and manage access to the DOI Drupal CMS content authors. Each DOI bureau and office is under a separate

acquisition plan for its use of DOI Cloud Drupal CMS platform and is responsible for their website content development and management ensuring PII data received through forms, blogs, questionnaires, emails and others is shared internally for authorized purposes. Individuals can reference specific program office pages or forms for a Privacy Act Statement, Privacy Notice or DOI Privacy Policy, or visit the DOI Privacy Program web page to view applicable PIAs and/or SORNs for more detailed information on how their PII will be used or shared.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

The purpose of DOI.gov is to disseminate information and engage the public so PII may be shared internally with DOI bureaus and offices to facilitate communication and respond to questions or requests by members of the public. Each DOI bureau and office is under a separate acquisition plan for its use of DOI Cloud Drupal CMS platform and is responsible for their website content development and management ensuring PII data received through forms, blogs, questionnaires, emails and others is shared for authorized purposes. Individuals can also reference specific program office pages or forms for a Privacy Act Statement, Privacy Notice, or DOI Privacy Policy, or visit the DOI Privacy Program web page to view applicable PIAs and/or SORNs for more detailed information on how their PII will be used or shared.

Each DOI bureau and office program official and data owner that uses Drupal or manages DOI.gov content is responsible for the information collected, used, shared and disseminated, and for ensuring its collection and use are only for authorized purposes. Data owners work with their bureau/office APOs to identify, assess, and manage privacy risks related to use of DOI.gov and Cloud Drupal CMS to meet Federal privacy requirements.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

Information received from website visitors or about user interactions may be shared with Federal agencies as authorized and required under Federal law, E.O., regulation or administration policy. This sharing is dependent on the circumstances, subject matter and legal requirements. In some cases, information may be shared with Federal law enforcement organizations as required by law, such as cases of defacement, threats or potential criminal activity that must be reported to appropriate Federal agencies. Due to the purpose and nature of the DOI.gov website and information dissemination and public outreach, there may be numerous forms, correspondence or services provided by bureau and offices programs that involve PII or are subject to the Privacy Act. Each bureau/office data owner or program official is responsible for ensuring PII data is shared with other Federal agencies only as authorized and for the purposes outlined in applicable program/office Privacy Act Statement, Privacy Notice, PIA and/or SORN. DOI data owners and program officials are responsible for the information they collect, use, share and disseminate, and ensuring it is only collected and used for authorized purposes. Data owners work with their bureau/office APOs to identify, assess, and manage privacy risks related to their use of DOI.gov and Cloud Drupal CMS. DOI, bureau, and office SORNs may be viewed at https://www.doi.gov/privacy/sorn.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

Each bureau/office data owner is responsible for ensuring PII data is shared for authorized purposes with Tribal, State and other local agencies. Information may also be shared with law enforcement as required by law. Each DOI bureau/office data owner or program official is responsible for ensuring the information they collect, use, share and disseminate using DOI.gov/Drupal CMS is for authorized purposes only and privacy notice is provided to individuals for specific programs including a Privacy Act Statement, Privacy Notice, applicable PIA and/or SORN describing how their PII will be shared. Data owners and program officials are responsible for working with their bureau APOs to identify, assess, and manage privacy risks related to specific information collections for use of DOI.gov and Cloud Drupal CMS system.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors are provided access to Drupal CMS and DOI.gov as authorized users to provide program support or technical support in managing the tool.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

No PII information is shared be shared with other DOI social media websites and third-party sites under contract with the Department.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Individuals are not required to provide their PII to visit the DOI.gov website. Individuals who visit DOI.gov may voluntarily submit PII through web forms, "Contact Us" feature, feedback forms, email, etc., to request information, make comments, register for notifications, or request services. Individuals can refer to the DOI Privacy Policy for information collected, opt-out options, for details on how to choose not to accept DOI cookies on their devices. However, it may take longer to navigate the Department's website if cookies are disabled.

Members of the public interested in signing up to receive updates on the Department's activities through email must consent to the DOI privacy policy prior to subscribing. Contact information provided will be used to deliver requested updates or to access subscriber preferences such as news, social media, and What we do. Individuals who voluntarily access third party links on the DOI.gov website receive a notice that they are leaving DOI.gov and are subject to the privacy policies of the third party website.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

Each DOI bureau/office data owner is responsible for meeting the requirements of the Privacy Act and providing a specific Privacy Act Statement or Privacy Notice for any applicable collection of PII, at the point of PII collection or on forms that collect PII from the public on their program website page.

☒ Privacy Notice: *Describe each applicable format.*

This PIA provides notice on the collection and use of PII for DOI.gov/Drupal CMS. DOI also provides a Privacy Policy on the DOI.gov website at https://www.doi.gov/privacy.

Privacy Notice may also be provided on specific program website pages. A Privacy Notice is available to individuals who sign up for the DOI email subscription notifications either directly on the DOI.gov page or link to the GovDelivery page. See the GovDelivery PIA for details on how PII is collected and used.

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

In general, the web content posted on DOI.gov is static, individuals' PII is not retrieved from the system. Notification emails are sent to the program official or owner of the webform whenever a new submission is received. Data is retrieved by the owner of the form by going into the results tab of the content management system to retrieve information. Program officials and data owners are responsible for ensuring any collection or use of PII specific to the program office meets requirements of the Privacy Act and other Federal privacy laws and policy.

I. Will reports be produced on individuals?

☐ Yes: *What will be the use of these reports? Who will have access to them?*
☒ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Data is collected directly from individuals filling out web forms, providing comments or answering questions and is presumed to be accurate at the time of collection. Each DOI bureau/office webform or content owner is responsible for managing their data and verifying its accuracy.

B. How will data be checked for completeness?

Data is collected directly from individuals filling out web forms, providing comments or answering questions and is presumed to be complete. Each DOI bureau/office webform or content owner is responsible for managing and verifying the completeness of their data.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data is collected directly from individuals filling out web forms, providing comments or answering questions and is presumed to be current. Each DOI bureau/office webform or content owner is responsible for managing their data and establishing processes to ensure it is current.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Records for the contents of DOI.gov may be covered by various record retention schedules, including:

- Departmental Records Schedule (DRS) 3.3.0008, Public Affairs Records created and maintained for the primary purpose of representing DOI to the public, state, local, and international governments, tribal nations, the news media and other private groups, which is approved by National Archives and Records Administration (NARA) (DAA-0048-2013-0008-0008). The disposition is permanent. The cut off starts at the end of the fiscal year in which the event occurred, or the publication was produced. Transfer non-electronic textual records to NARA 15 years after cut-off.
- DRS 3.5.0011 through 0015 – Policy Related Special Media Records, these records cover Photography and Negatives, Motion Pictures, Video, and Audio Recordings and Posters. DAA-0048-2013-0011 through 0015. The disposition is permanent. The cut off starts at the end of the fiscal year in which the event occurred, or the publication was produced. Transfer records of other media types to NARA 3 years after cut-off.
- DRS 1.1.0001 DAA-0048-2013-0001-0001, these records encompass all DOI activities that support a program office internal operation not associated with human resources, payroll, financial accounting, procurement and information technology. The disposition

is temporary. The cut-off starts at the end of each presidential administration or at the end of the fiscal year. Destroy 3 years after cut-off.

Retention schedules vary based on the type of record, subject matter, and needs of the specific program/office. Each program official and data owner is responsible for managing their own records and following the appropriate retention schedule for the records created for their specific programs/activities in accordance with the Federal Records Act, Departmental and bureau/office policy.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

The approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA Guidelines and Departmental policy. Each program official and data owner is responsible for disposing of or purging their data according to approved DOI disposition methods.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a risk to the privacy of individuals due to the personally identifiable information that may be provided during interaction with DOI on DOI.gov or voluntarily provided through web forms, the Contact us feature, and communications through email. These risks include lack of notice, lack of opportunity to consent to collection or use of PII, unauthorized access, use or sharing of PII, and collecting more information than needed or retaining it longer than necessary. Individuals visiting the DOI.gov website are cautioned to refrain from including sensitive information in communications. Visiting DOI.gov does not require PII, however, personal contact information such as email address may be provided by individuals to interact with DOI. DOI will use this information to respond to a question or request made by the individual. The DOI Privacy Policy is available on DOI.gov for more information on the information that is collected when individuals visit the DOI.gov website and how this information will be used to interact with users and internally for site management purposes.

There is a risk that individuals may not receive adequate notice for the collection of their PII or have an opportunity to consent to its collection and use. This risk is mitigated through various notice and consent mechanisms. The DOI Privacy Policy provides information to visitors to DOI.gov on the information that is collected when they visit the DOI.gov website and how this information will be used and shared, how DOI uses social media, how to opt-out of the use of cookies, the linking policy, and other information that allows individuals to make informed decisions. Individuals are provided a Privacy Notice for any collection of PII and a specific Privacy Act statement for any web form or information collection that is subject to the Privacy Act. Notice is also provided through this privacy impact assessment and any applicable SORNs published for the specific programs that collect PII. The DOI Privacy Policy page includes contact information for privacy officials and provides guidance to individuals on how they can

submit a Privacy Act request for access or amendment of records, or a complaint or request for redress, to Departmental, and bureau and office privacy officials.

There is no direct data transfer between DOI.gov and other DOI websites on the Drupal CMS platform. Per DOI policy, IBM conducted a security assurance assessment on Cloud Drupal CMS to ensure the risks are properly identified and the selected and required security controls are implemented. The acquisition contract between DOI and the vendor includes specific security and privacy provisions on the vendor's obligations to ensure the vendor's security and privacy protection controls and measures are in strict compliance with the federal laws and regulations. DOI also conducted a formal Assessment and Authorization on DOI's use of the Cloud Drupal platform and DOI.gov before issuing the Authorization to Operate (ATO) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and National Institute of Standards and Technology (NIST) standards. DOI.gov and Drupal CMS are rated as a FISMA moderate systems. Each DOI bureau and office is under a separate acquisition plan for its use of DOI Cloud Drupal CMS platform and each is responsible for their website content development and management activities, protecting individual privacy, and complying with Federal laws and policies for the information collected, processed, and transmitted through DOI.gov.

There is a risk that some DOI bureau or office DOI.gov sub-page webforms may collect more PII than is needed or collect PII that is sensitive, or that data transmitted on DOI.gov or stored on Drupal CMS may be inappropriately accessed or used for unauthorized purposes. The program officials and data owners are responsible for ensuring only minimum PII needed is collection and that collection is authorized to support a mission or business need in accordance with the Privacy Act, other Federal law and policy, and DOI privacy policy. To protect the privacy of the users and the information transmitted by DOI website, DOI implemented a series of technical, administrative and physical controls, including encryption to secure transmissions to prevent interception or altercation. Each Data Owner is responsible for ensuring only personnel with the business need-to-know are authorized to access and process Drupal CMS data based on least privilege principles and DOI policy. In addition, each program official and data owner is responsible for ensuring all staff complete DOI's annual security, privacy, record and role-based training and sign the DOI Rules of Behavior (ROB) prior to accessing DOI.gov and Drupal CMS. The DOI Web Standards Handbook requires that owners of content posted on DOI.gov be accountable for and comply with all Federal laws and regulations to ensure content and format serve the needs of the public and protect privacy rights of the individuals. The DOI Web Council provides oversight on the DOI website activities, a web manager is designated as the responsible official for meeting DOI's compliance requirements.

There is a risk that data from webforms may be stored for longer than necessary in Drupal CMS. Each data owner is responsible for ensuring information collected and stored in Drupal CMS is maintained, protected, and destroyed in compliance with a NARA approved records retention schedule and all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. Data owners have the option of selecting a timeframe of when data may be deleted in 1 day, 7 days or 30 days. Drupal CMS also has an option to not collect data.

DOI maintains accounts on third-party websites and applications. There is a risk that this use and the display of third-party links on DOI.gov may pose privacy risks to visitors. Links to third-party sites are used to facilitate citizen engagement and open dialogues with DOI, and a message box will pop up to notify visitors they are leaving DOI.gov and allow them to either consent or deny following the link before they proceed further. DOI does not control what these third-parties do with information they collect and the DOI Privacy Policy does not cover these external websites. Where an individual voluntarily chooses to access a third-party link through the DOI.gov website, the individual is subject to the Privacy Policy of that third-party website.

There is a risk related to the use of website measurement and customization technologies, also known as "cookies", on DOI.gov. Cookies are small bits of text that a website transfers to a computer to allow it to remember information about a session with the website. DOI uses cookies to improve the user experience while navigating the website or to customize user preferences while interacting with DOI.gov. Session cookies may be used during a single session and are removed when the user ends the session or leaves the site. Persistent cookies may be saved on the user's hard drive and are used between visits to save customized preference settings for future visits, manage survey requests, or conduct website analytics to improve the website. The use of these cookies uniquely identify a browser but do not identify individual visitors or collect PII. DOI.gov does not use persistent cookies that collect PII. The DOI Privacy Policy provides instructions for visitors to DOI.gov on how individuals may choose to opt-out of this use and disable cookies in their browsers.

DOI uses GovDelivery to manage individual subscriptions for email notifications. Visitors to DOI.gov and members of the public interested in receiving updates on the Department's activities via email are redirected to GovDelivery to voluntarily subscribe for email notifications based on their interests. Contact information provided will be used to deliver requested updates or to access subscriber preferences such as news, social media, and What we do. Individuals may unsubscribe at any time. DOI conducted a separate PIA for use of GovDelivery, which may be viewed at https://www.doi.gov/privacy/pia.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes

DOI.gov uses Drupal CMS to engage with the public on DOI's diverse missions and activities by creating, editing, uploading and managing content for its public facing website. Each DOI bureau/office is responsible for managing their content according to DOI policy and applicable Federal laws.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Not Applicable. DOI.gov and Drupal CMS do not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

Access is controlled through user account management and authentication with the DOI Active Directory system. Only authorized DOI personnel will have access to the system. Each bureau/office System Administrators for DOI.gov have access rights to the system to perform system administration and can view or delete certain data for troubleshooting purposes. Public users of DOI.gov can view all published content (webpages, records, audio/video, etc.) for informational purposes on DOI's mission and activities.

The internal authors of DOI.gov can access and modify the content they own or have been granted edit privileges.

The developers of DOI.gov have access rights to the artifacts of the website for web development purposes. DOI currently contracts with these developers to design its website. They have access to all of the content on the DOI.gov website and have completed the necessary vetting process in order to obtain a PIV card.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Users' access to data is based on the principle of least privileges. Users will be granted access to data based on their organization's needs. Each office determines a user's level of access and managers asses data restrictions independently. DOI.gov implements technical controls to ensure users do not have access to data outside of their assigned roles. NIST SP 800-53 access controls are assessed on an annual basis to certify data restrictions are implemented correctly.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved in the design, development and maintenance of the system. Privacy Act clauses are included in the contract with IBM. Contractors also have access as authorized users.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*

☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system does not monitor individuals. The DOI internal users' logon activities are offloaded to DOI Active Directory (AD) through DOI's centralized user account management process.

M. What controls will be used to prevent unauthorized monitoring?

Each bureau/office is responsible for granting access to their content owners. The DOI and IBM support Drupal-based application management. Component security relevant information is restricted to Security Administrators and is segregated based upon user and group access. Group memberships have been designed and implemented using Role Based Access Control (RBAC) methodologies to restrict access to authorized personnel. Group memberships are designed by function, an individual is assigned to their functional group based on their role within the organization. All system users must complete privacy and security training and testing in order to access DOI.gov and Drupal CMS based systems and sign DOI Rules of Behavior. DOI.gov traffic is encrypted by default utilizing a FIPS 140-2 validated encryption module to protect sensitive information residing on digital media during transport.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☐ Key Guards
☐ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☒ Other. *Describe*

Drupal CMS inherits the physical controls implemented by IBM on its operation sites. DOI.GOV inherits the physical controls of the boundary where DOI.GOV domain is hosted.

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall

☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☒ Other. *Describe*

Drupal CMS: Personnel guidance is provided from IBM for security-based services. System policy provides guidance based on IBM system personnel policies.

Automated tools and analysis are provided by system management functions for regulatory compliance with system monitoring. All tools used for Drupal such as IBM supports Intrusions Detection System and Intrusion Prevention System with near-time analysis.

Information input restrictions are based upon access and authorization to the system. IBM personal have access to ensure that local systems are managed appropriately and that system functions such as website publishing information is delegated to the appropriate information DOI resources.

DOI.GOV: Local users for DOI follow inherited DOI policies for personnel system controls.

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site (cloud provider)
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data (cloud provider)
☒ Mandatory Security, Privacy and Records Management Training
☒ Other. *Describe*

Drupal CMS: Systems acquired are managed as part of DOI based system requirements. This is inherited as part of systems that are deployed for the IBM Infrastructure as a Service and Platform as a Service accredited Cloud services.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The DOI Web Manager, Office of Communications, is the Information System Owner and the official responsible for the oversight and management of the DOI.gov security controls for the protection of any information processed and transmitted through DOI.gov in Drupal CMS. The Information System Owner and the Information System Security Officer (ISSO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies.

DOI bureau/office content owners and program officials are responsible for protecting individual privacy for the information collected, maintained, used and transmitted by the system, and meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act complaints and requests for notification, access, and amendment, in consultation with DOI privacy officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The DOI.gov/Drupal CMS Information System Owner is responsible for oversight and management of the DOI.gov/Drupal CMS security and privacy controls, and for ensuring to the greatest possible extent that DOI.gov/Drupal CMS is properly managed and that all access to DOI.gov/Drupal CMS data has been granted in a secure and auditable manner. The DOI.gov/Drupal CMS Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.

DOI bureau/office program data in DOI.gov/Drupal CMS is under the control of the bureau/office program official, webform or data owner. Each DOI bureau/office is responsible for the management of their own data and the reporting of any potential loss, compromise, unauthorized access or disclosure of data resulting from their activities or management of the data to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established DOI procedures.