



## 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:** Enterprise Hosted Infrastructure (EHI)

**Bureau/Office:** Office of the Chief Information Officer

**Date:** October 5, 2016

**Point of Contact:**

Name: Teri Barnett

Title: Departmental Privacy Officer

Email: Teri\_Barnett@ios.doi.gov

Phone: 202-208-1605

Address: 1849 C Street NW, Mail Stop 5545 MIB, 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 Enterprise Hosted Infrastructure (EHI) boundary is a General Support System (GSS) that hosts the Enterprise Active Directory (EAD) and Enterprise Hosted Service (EHS). EHI provides Enterprise authentication, authorization, security, Domain Name Services (DNS), Synchronization services, and Public Key Infrastructure (PKI) services for the Department, Bureaus, and Offices utilizing Microsoft Active Directory (AD) services. EHI utilizes account information provided by the user to implement access control measures and rights management to ensure access to DOI's information and systems are secure. EHI is also used by other applications within DOI to perform identification and authentication on



user requests to the DOI BisonConnect email system and Microsoft Office SharePoint Service (SharePoint). Providing a single directory service across all of DOI eliminates redundancies, standardizes configurations, and creates a more secure environment by containing access control and authentication services within one domain directory system.

The EHS system includes SharePoint, which provides a Web page user interface and enterprise collaboration and project management services. Hosted SharePoint content sites are owned and administered by personnel from various subscribing DOI bureaus and offices. SharePoint users may post information, documents, spreadsheets, PDFs, graphics, etc. to share or collaborate via a secure encrypted internal website.

Active Directory user account information includes names, passwords, and login time, data, and locality, and is used to authenticate user access and actions within EHI.

DOIAccess is an internal DOI application that ensures compliance with Homeland Security Presidential Directive -12 (HSPD-12) and National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 201 standards by providing an automated, standard Personal Identity Verification process that integrates Human Resources, Personnel Security, Physical Security and Information Technology business processes. See the DOIAccess PIA for assessment of privacy risk.

See F below for additional applications in the EHI GSS.

### **C. What is the legal authority?**

5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004; E-Government Act of 2002, as amended; 110 Departmental Manual 18.

### **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*

### **E. Is this information system registered in CSAM?**

*The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.*



Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000667 Enterprise Hosted Infrastructure (EHI)

No

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

<b>Subsystem Name</b>	<b>Purpose</b>	<b>Contains PII (Yes/No)</b>	<b>Describe If Yes, provide a description.</b>
<b>Enterprise Directory Services</b>	Authoritative source of user identification and authentication information for DOI Enterprise.	Yes	Usernames, and general contact information associated to user.
<b>EHS SharePoint</b>	Internal –Information management and sharing	Yes	EHS content databases (SharePoint) may have information identifiable to an individual however the data is owned and maintained by the program offices who manage their sharepoint sites.
<b>Extranet Sharepoint</b>	External-Information management and sharing	Yes	Extranet Sharepoint content databases may have information identifiable to an individual, however the data is owned and maintained by the program offices who manage their sharepoint sites.
<b>SQL Database Services</b>	Data Storage	Yes	SQL Database Services may have information identifiable to an individual, however the data is owned and maintained by the program offices who utilize the service.



<b>Storage Area Network</b>	Data Storage-Record Retention	Yes	The Storage Area Network may have information identifiable to an individual. However, any data stored is the responsibility of the program official.
<b>Microsoft Project Server</b>	Project scheduling and budget formulation	No	This application supports project scheduling.
<b>United Communications Infrastructure</b>	Communication channels used within DOI. (Link, ArcGIS, WebEOC, Safe Talk, Radio Technology Servers, Team Foundation Servers)	No	Hosted applications that provide communications services. See specific PIAs for these applications.
<b>DOIAccess</b>	DOIAccess ensures compliance with HSPD-12 and FIPS 201 standards by providing an automated, standard Personal Identity Verification business process across DOI	Yes	Personal Identity and authentication data used to identify individuals and used to grant access within the DOI enterprise. See DOIAccess PIA for assessment of privacy implications.

**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)*

DOI-47: “HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS), which is currently being revised.

No

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

Yes: *Describe*

No



## Section 2. Summary of System Data

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

- |  |   |   |
|--|---|---|
| <input checked="" type="checkbox"/> Name   | <input type="checkbox"/> Religious Preference   | <input type="checkbox"/> Social Security Number (SSN)   |
| <input type="checkbox"/> Citizenship       | <input type="checkbox"/> Security Clearance     | <input type="checkbox"/> Personal Cell Telephone Number |
| <input type="checkbox"/> Gender            | <input type="checkbox"/> Spouse Information     | <input type="checkbox"/> Tribal or Other ID Number      |
| <input type="checkbox"/> Birth Date        | <input type="checkbox"/> Financial Information  | <input type="checkbox"/> Personal Email Address         |
| <input type="checkbox"/> Group Affiliation | <input type="checkbox"/> Medical Information    | <input type="checkbox"/> Mother's Maiden Name           |
| <input type="checkbox"/> Marital Status    | <input type="checkbox"/> Disability Information | <input type="checkbox"/> Home Telephone Number          |
| <input type="checkbox"/> Biometrics        | <input type="checkbox"/> Credit Card Number     | <input type="checkbox"/> Child or Dependent Information |
| <input type="checkbox"/> Other Names Used  | <input type="checkbox"/> Law Enforcement        | <input type="checkbox"/> Employment Information         |
| <input type="checkbox"/> Truncated SSN     | <input type="checkbox"/> Education Information  | <input type="checkbox"/> Military Status/Service        |
| <input type="checkbox"/> Legal Status      | <input type="checkbox"/> Emergency Contact      | <input type="checkbox"/> Mailing/Home Address           |
| <input type="checkbox"/> Place of Birth    | <input type="checkbox"/> Driver's License       | <input type="checkbox"/> Race/Ethnicity                 |
- Other: *Specify the PII collected.* Username, password hash values, HSPD-12 authentication, official email address and phone number, duty station address, official title of DOI employees and contractors, and supervisor name.

### 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
- Other: *Describe*

AD user data is provided by interface with DOIAccess and is also provided by individual users during the account creation or updating process. Each Bureau or Office has their own process and forms to



request and provision user accounts within AD. AD continuously updates data across the DOI domains.

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

PII is used in the creation and administration of DOI user accounts. EHI provides access control and user authentication for services, applications, and other network resources across the DOI environment using the provided information.

**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.*

DOI.net AD root will replicate user account information between Bureau/Office domain controllers for the purpose of network access enforcement.

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

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

The HSPD-12 program is a government-wide requirement managed by the General Services Administration and is subject to Federal requirements for participating agencies that involve sharing of data - see government-wide system notice GSA/GOVT-7: Personal Identify Verification Identity Management System, for additional information sharing activities. Some information may be shared with other Federal Agencies as authorized pursuant to the routine uses contained in the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

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

Information may be shared with Tribal, state, or local agencies as authorized pursuant to the routine uses contained in the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

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

Information may be shared with contractors who perform services or otherwise support DOI activities related the EHI, and as authorized pursuant to the routine uses contained in the DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

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

**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.*

Information is voluntarily provided by employees in order to obtain access to the DOI network and information systems. Users have the opportunity to consent during the onboarding process and verification of approval to work is required to enforce access controls across the DOI network. If users decline to provide the required information upon employment at DOI they will not be given access to the network and may be unable to perform their duties.

- 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.*

Data on new users is provided by DOIAccess. In some cases users may request a new or updated account be created within the DOI domain through a form that will contain a Privacy Act Statement (PAS). Each Bureau/Office has their own process and templates for provisioning accounts. The following (PAS) will be provided for their processes and related forms.

Privacy Act Statement

Authority: The collection of information is authorized under 5 U.S.C. 301; the Paperwork Reduction Act of 1995 (44 U.S.C. 3501); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504); and Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004.

Purpose: DOI will use this information to create and activate user accounts within the DOI domain and provide a common authoritative directory service for the purpose of ensuring the security of DOI computer networks and information, and protecting them from unauthorized access, tampering or destruction.

Routine Uses: The information will be used by and disclosed to DOI network administrators for the purpose of managing user accounts, to authenticate and verify that all persons accessing DOI computer networks, resources and information are properly authorized to access them and providing assistance to users in the event of a security or configuration error.

Disclosure: Furnishing this information is voluntary; however, failure to furnish the requested information will prevent the creation and activation of a user account. This will prevent the user from accessing or authenticating to the DOI network.

- Privacy Notice: *Describe each applicable format.*



Notice is provided through publication of this PIA and the DOI-47: “HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) system of records notice.

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.).**

Data is retrieved using AD native tools by name, workstation name, and AD group. SharePoint offers a search function which can be used to retrieve data stored within the environment. Document names and keywords can be used to search for documents. There is no function within SharePoint to search on usernames or user information.

**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 from DOI records, and is not collected from other sources.

**B. How will data be checked for completeness?**

Specific account attributes within EHI can be updated upon request of the user which would be primarily contact information. The specific User identification (UID) information cannot be changed. SharePoint data owners are responsible for verifying and updating the information relevant to the service to which they subscribe. Individual Bureaus and Offices have processes in place to review and update information contained within each individual SharePoint site.

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

Certain updates may take effect via the AD system updates, however; it is up to the individual to update their contact information and update data in any application and/or system that is hosted within EHI. DOI provides the My Account (<https://myaccount.doi.gov>) site where users can maintain and update their work related contact information. Users are notified that it is their responsibility to ensure their information is up to date. As a function of AD, all data related to user access is continuously synchronized across the entire system.



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

Records maintained in AD are retained in accordance with Departmental Records Schedule (DRS) – Administrative schedule 1.4A.1 - [0013] Short Term IT Records - System Maintenance and Use Records, which has been approved by the National Archives and Records Administration (NARA). These records encompass IT files described that are not needed for extended retention. Records are characterized by being necessary for day-to-day operations but no longer term justification of the bureaus/offices activities. In general, EHI directory configuration data is stored online 30 days on their respective servers and stored offline for 12 months. As a function of AD, all data related to user access is continuously synchronized across the entire system. Therefore active accounts are retained within the system and once user accounts are deactivated or terminated the associated records will be retained for the time periods described above. Records maintained on the SharePoint are the responsibility of DOI program officials. Retention periods will vary, depending on the bureau, office, program and subject matter of the records maintained and needs of the organization.

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

Once user accounts are terminated in the system, the records are removed in accordance with the DRS and other applicable bureau/office records retention schedules. Reports are not generated. Procedures for disposition of the data stored in individual applications will vary by application. When a user account is disabled or terminated in the EHI, all access will be denied since the user will no longer have the ability to log onto or authenticate to the network. The EHI user objects can be set to automatically expire at a given date to ensure that a user does not have access past the period of performance or contract. When the account is disabled, all access to the network and all EHI systems are explicitly denied and all attempts to gain access are logged. Approved disposition methods include erasing, degaussing, deleting, and shredding in accordance with the appropriate records schedule, DOI records policy and NARA guidelines.

**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 minimal privacy risk to individuals due to the limited information contained in the AD system and the mitigating controls implemented to protect data. Most of the PII includes employee name, username, work email address, work phone number, duty station address, and official title of DOI employees and contractors, and the work related PII, such as contact information, duty station, and title, is not considered sensitive. System permissions and access controls are in place to limit system access to only those authorized individuals with a need to know the information to perform official functions.

EHI has undergone a formal Assessment and Authorization and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards. EHI is rated as FISMA moderate based upon the type



of data and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the PII contained in the system.

The EHI GSS has developed a System Security Plan based on NIST guidance and is part of a Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with policy and standards. Additionally, vulnerability scans are routinely conducted on the EHI GSS to identify and mitigate any found. Security and privacy awareness training is required for all DOI employees and information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter, and sign the DOI Rules of Behavior. Security role-based training is also required for security personnel and officials with special roles and privileges.

DOI complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any EHI equipment. The use of DOI IT systems, including EHI, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Access to administrative functions is strictly controlled and can only be granted by EHI Enterprise Managers. Additionally, users must be included in security groups assigned to a SharePoint resource in order to access that particular resource. Users must obtain authorized access by SharePoint administrators (who will be delegated administrative rights by data owner and/or system managers) to access resources within the SharePoint environment. It will be the responsibility of users of the SharePoint services to adhere to the system rules of behavior regarding the types of information that should not be stored in the EHI sub-systems or applications.

## 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: *Explanation*

Data is required for the purposes of providing Enterprise access control and management to allow seamless interaction between DOI and Bureaus while still maintaining the appropriate level of security.

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 since EHI does not generate new data.

**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.*

Data gathered from Bureaus is consolidated into the DOI AD, which is used to authorize access to individual users throughout the enterprise and to manage system and application level access. Data contained within AD is controlled by permissions and access is only granted to a few individuals with the correct level of permissions to view the data.

- 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* Users and contractors will have access to their own information, and in some cases a limited subset of other users based on mission, system, and application management needs.

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

Access to data will be restricted through AD permissions and access controls. System administrators will have access based on a need to know and mission accomplishment.

**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?*

The standard Privacy Act clauses are included in the contracts.

- 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* As part of the security monitoring and management of the system all user actions taken on EHI resources are audited and can be reviewed by Enterprise and Domain administrators. This information includes items such as: failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.

- No

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

As part of the security monitoring and management of the system all user actions taken on EHI resources are audited and can be reviewed by Enterprise and Domain administrators. This information includes items such as: username, login date/time/location, failed login/access attempts, changes in user permissions, and failed AD services associated with user authentication.



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

DOI complies with NIST and other Federal requirements for data security as part of a formal program of assessment and authorization, and continuous monitoring. Monthly scans of the network are performed to ensure that changes do not occur that would create an exposure or weakness in the security configuration of any EHI equipment. The use of DOI IT systems, including EHI, is conducted in accordance with the appropriate DOI use policy. IT systems maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular basis and any suspected attempts of unauthorized access or scanning of the system are reported immediately to IT Security.

Access to administrative functions is strictly controlled and can only be granted by EHI Enterprise Managers. Additionally, users must be included in security groups assigned to a SharePoint resource in order to access that particular resource. Users must obtain authorized access by SharePoint administrators (who will be delegated administrative rights by data owner and/or system managers) to access resources within the SharePoint environment. It will be the responsibility of users of the SharePoint services to adhere to the system rules of behavior regarding the types of information that should not be stored in the EHI sub-systems or applications. Also, all users must complete IT security and privacy awareness training, as well as role based training on an annual basis and before being granted access, and sign the DOI Rules of Behavior.

### **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*

(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*

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits
- Backups Secured Off-site
- 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
- Mandatory Security, Privacy and Records Management Training
- Other. *Describe*

**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 Office of the Chief Information Officer, Chief, End User Services serves as the EHI Information System Owner and the official responsible for oversight and management of the EHI security and privacy controls for the EHI system. The Information System Owner and the Logical Security Files Privacy Act System Manager are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in EHI. The Privacy Act System Manager is responsible for responding to Privacy Act requests and complaints 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 EHI Information System Owner is responsible for oversight and management of the EHI security and privacy controls, and for ensuring to the greatest possible extent that EHI data is properly managed and that all system access has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and US-CERT within 1-hour of discovery in accordance with Federal policy and established procedures.