

**Department of the Interior**  
**Enterprise Hosted Infrastructure**  
**Privacy Impact Assessment**

October 21, 2009

**Name of Project:** Enterprise Hosted Infrastructure (EHI): (formerly Enterprise Hosted Services (EHS) and Enterprise Active Directory (EAD)).

**Bureau:** OS Enterprise Infrastructure Division (EID)

**Project's Unique ID (Exhibit 300):** 010-00-02-00-03-2041-00

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

**Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.**

**A. CONTACT INFORMATION:**

Departmental Privacy Office  
Office of the Chief Information Officer  
U.S. Department of the Interior  
202-208-1605  
DOI\_Privacy@ios.doi.gov

**B. SYSTEM APPLICATION/GENERAL INFORMATION:**

- 1) **Does this system contain any information about individuals** *{this question is applicable to the system and any minor applications covered under this system}?*

Yes.

The following information is stored:

1) The EHI GSS is comprised of 2 former independently assessed General Support Systems (GSS): the EAD and the EHS. The EHS GSS includes the Microsoft Office SharePoint Server (MOSS), hereafter referred to as SharePoint. The EHI GSS will provide several hosted services and applications which will provide enterprise identification and authentication services, and SharePoint servers with a Web page user interface to provide collaboration and project management services. These shared resources allow data owners and users to post information (documents, spreadsheets, PDFs, lists, graphics, etc.) they wish to share, or collaborate on via an encrypted internal website. Data owners and users will subscribe to services provided by the EHI GSS. Subscriber data may include, but will not be limited to, any Department of Interior bureau and office data pertinent to geographical information systems, radio wave analysis, project planning, personnel, human resources, capital planning, and any resources that SharePoint subscribers of the service post to their site.

2) The EHI will contain DOI Employees and Contractors business contact information (Telephone/address/email) as well as partner account information (imported from Enterprise Active Directory on a routine schedule and also stored in the SharePoint system. DOIAccess will also maintain personal information about employees, contractors, and partners. Changes to the user's information in Enterprise Active Directory will overwrite the stored information when the next import occurs.

All users subscribing to EHI services will be required to electronically sign Rules of Behavior statements which will at a minimum state their adherence to all EHI PIA security and privacy requirements. The EHI SharePoint infrastructure is considered independent of the hosted applications/ sites and does not own any of the hosted data.

3) User Account Information (user account names, password, and login time/date/locality) to Active Directory and external systems using Active Directory authentication (which includes but is not limited to all services within EHI)

4) Audit logs (login time/date/locality) are stored in the server system logs and also stored in the NetIQ Security Manager system.

- a. **Is this information identifiable to the individual**<sup>1</sup>*{this question is applicable to the system and any minor applications covered under this system}*? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, Sections C through F can be marked not applicable. If YES complete all sections for system and any applicable minor applications).

Yes.

Work address and telephone numbers are identifiable to the individual.

---

<sup>1</sup> "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

User names are identifiable to the employee/contractor name. Password files are housed in an encrypted database.

- b. Is the information about individual members of the public** *{this question is applicable to the system and any minor applications covered under this system}*? (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).

No.

- c. Is the information about employees** *{this question is applicable to the system and any minor applications covered under this system}*? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes

**2) What is the purpose of the system/application?**

The system provides Active Directory Root Services administration for the DOI.NET Active Directory Infrastructure, offers scalable storage solutions, and facilitates an information sharing platform for cross bureau collaboration.

**2a) List all minor applications and sub-systems that are hosted on this system and covered under this privacy impact assessment:**

SUB-SYSTEM/ MINOR APPLICATION NAME	NIST 800-60 DATA TYPES
Enterprise Active Directory	Information Security Information Type
Symantec Backup Exec	Information Management Information Type
Microsoft Office SharePoint Server (MOSS)	Information Management Information Type
Microsoft Office SharePoint Services	Information Sharing Information Type
Unified Communication Infrastructure (UCI): Microsoft Exchange, Blackberry Enterprise Services, and Office Communications Services	IT Infrastructure Maintenance Information Type
Team Foundation Server: SourceSafe	System Maintenance Information Type
Team Foundation Server: SourceSafe	Development Information Type
Storage Area Network	Record Retention Information Type
Project Portfolio Management Services	Budget Formulation Information Type
Interior Operational Center (IOC): ArcGIS, WebEOC, SafeTalk	Disaster Preparedness and Planning Information Type

<b>Radio Technology Services</b>	<b>IT Infrastructure Maintenance Information Type</b>
<b>DOIAccess: Identity and Access Management Information System</b>	<b>Personal Identity and Authentication Information Type</b>
<b>SQL Database Services</b>	<b>Information Management Information Type</b>

**3) What legal authority authorizes the purchase or development of this system/application?**

Pub. L. 107-347 (E-Government Act of 2002, as amended). 110 Departmental Manual 18.

**C. DATA IN THE SYSTEM:**

**1) What categories of individuals are covered in the system?**

Department of Interior Employees and Contractors as well as partners (students, interns, emeritus, seasonal personnel, union representative, tribal user).

**2) What are the sources of the information in the system?**

Source of the information is from the individual, from each business' Active Directory administrator, and any DOIACcess sponsors for the DOIAccess account creation process who populates each employee and contractor's work contact information or user provided information. Username is generated by the System administrator.

**a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

The information for individual users may be imported directly from Enterprise Active Directory which serves as the single authoritative source for user information across Department of Interior bureaus and offices. Once authenticated, users information can also be retrieved from SharePoint.

EHS content databases (SharePoint applications) may have information identifiable to an individual; however, the hosted data is not assessed in scope.

**b. What Federal agencies are providing data for use in the system?**

None except for the Department of Interior for its internal use.

**c. What Tribal, State and local agencies are providing data for use in the system?**

Bureau of Indian Affairs (BIA) and Bureau of Indian Education users may provide data for use in the system; however SharePoint data is not assessed in scope and BIA domain controllers are not included within the EAD boundary (only the root and EIS DC's are assessed)

**d. From what other third party sources will data be collected?**

The EHI system will provide secure and facilitative services for collaboration sites, project management planning, continuity of operations data, and network share databases, etc. for users from all bureaus and offices to share documents and collaborate on projects. Additionally, the EHI system will offer a long term storage service for backup and recovery data for any bureau or office that owns/ leases space on that service. All SharePoint users must agree and sign a Rules of Behavior agreement prior to being given access to any of the sub-systems or hosted application services in the EHI system.

**e. What information will be collected from the employee and the public?**

Work phone number, address, title, and email contact information from Department of Interior Employees and contractors will be stored in the Enterprise Active Directory system, which the EHS system will use for access and authorization credentials. Certain EHI SharePoint applications will collect user account information (login date/time/locality and changes made to data with timestamps) as well as other user data; however the hosted data is not assessed in scope.

**3) Accuracy, Timeliness, and Reliability**

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

There are no other sources other than Department of Interior records.

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

EHI (particularly SharePoint) data owners are responsible for verifying and updating the information relevant to the service to which they subscribe.

**c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

Certain updates may take effect via the Active Directory system updates, however; it is up to the individual to update his/her contact information and update data in any applications and/or systems that are hosted within the EHI.

**d. Are the data elements described in detail and documented? If yes, what is the name of the document?**

Yes. The data elements are described in the Certification and Accreditation documents associated with the Enterprise Hosted Services and Enterprise Active Directory Systems, now being consolidated for uniform consideration.

**D. ATTRIBUTES OF THE DATA:**

**1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

**2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No.

**3) Will the new data be placed in the individual's record?**

No.

**4) Can the system make determinations about employees/public that would not be possible without the new data?**

No

**5) How will the new data be verified for relevance and accuracy?**

N/A

**6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Data in the EHI is not being consolidated; however the data can only be accessed with a valid user ID and password and users must be authorized and placed into specific administrative groups to view or modify any user data.

**7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

N/A

**8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Data can be retrieved using LDAP (Lightweight Directory Access Protocol) or Active Directory native tools by the System Administrator. Data can also be retrieved by Exchange and SharePoint. Data can also be retrieved by name of individual by using the START/SEARCH function on DOI Workstations.

EAD does not have a need for the contact information on the Active Directory infrastructure and does not normally retrieve the data. Each of DOI's various bureau's Active Directory Child Domains, are outside the boundary of the EAD system boundary and each bureau's System Administrator maintains their own bureau's information and uses that information differently. But due to the architecture of DOI's Active Directory infrastructure, EAD receives a copy of all user information from all the bureaus.

Within the SharePoint application, using the search center, information can be searched for where a specific user was the author, or last one to modify it. Additionally, a search for a particular individual can be run, but the results will only return the information imported from Enterprise Active Directory (account name, email address, etc.) as previously discussed.

Data can be filtered and retrieved using the SharePoint application out the box Customizable Search Center, Web Service search, etc. However, when a user conducts a search the search results are parsed against that user's credentials and the access control lists for the content. The query results will only be shown to users who have access to that information.

**9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

The EHI GSS will not produce reports on individuals, but SharePoint application can provide basic website statistics and usage (who browsed to what page or file) and audit reports of user actions. Only personnel designated as administrators for the site will have access to this information. However, as mentioned above, search query results by site administrators will only be shown to those who have access to that information. Within the EAD sub-system, tabular reports that contain aforementioned populated attributes can be generated. There is no current use of these reports as majority of the fields are not populated. No reports are being created.

**10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

It is up to the individual bureaus whether to populate any of the contact data. The only mandatory field is the assigned logon username (assigned via Enterprise Active Directory. Individuals cannot decline to have their login activity stored.

**E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:**

**1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Depending on the sub-system within the EHI GSS, the EHI will be hosted at multiple sites, but not every sub-system will be hosted at the same multiple sites.

**2) What are the retention periods of data in this system?**

EAD active data is stored until employee or contractor user accounts are terminated, as per GRS 20.

The EHS and all applications hosted on it will be covered by records retention schedules as a part of the OS Records Schedule approved by the National Archives and Records Administration. Retention periods will vary, depending on the content and purpose of the applications.

In general, EHS data is stored online for 30 days on their respective servers while systems and applications and it is stored offline for 12 months. Enterprise Active Directory data is stored until employee or contractor user accounts are terminated.

**3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Once user accounts are terminated in the system, the records are removed, as per GRS 20. There are no reports being 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 Enterprise Active Directory, all access to the EHS system will be denied since the user will no longer have the ability to log onto or authenticate to the network or the Enterprise Active Directory domain.

The Enterprise Active Directory user objects can be set to automatically expire at a given date (such as the end of a contract) 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 therefore all EHS systems is explicitly denied and all attempts to gain access are logged.

- 4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

- 5) **How does the use of this technology affect public/employee privacy?**

N/A

- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No.

- 7) **What kinds of information are collected as a function of the monitoring of individuals?**

All EHI resource users actions to and from certain services can be reviewed for auditing purposes.

- 8) **What controls will be used to prevent unauthorized monitoring?**

Access to these administrative functions is strictly controlled and can only be granted by the EHI System Manager. 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 owners and/or system managers) to access resources within the SharePoint system. Additionally, 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 (i.e. personal health information, social security numbers, home contact info, and other data that is considered personally identifiable or sensitive information). Additionally, all users must complete IT Security Awareness Training before being granted access, and annually thereafter. Finally, all users sign Rules of Behavior and receive supervision while operating in agency offices.

- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

The EAD sub-system is covered under Interior, DOI-47: "HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS)". The EHS sub-system components are not covered by a Privacy Act system of records notice either because it does not contain personal information protected by the Privacy Act, or if some incidental information is included, it is not routinely accessed by a personal identifier. Individual applications may, however, contain personal information protected by the Privacy Act with plans for routine accessing by personal identifiers, and thus may require their own privacy impact assessments and system of records notices, as referenced in their DEAR entries.

- 10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

N/A

**F. ACCESS TO DATA:**

- 1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

Only the Enterprise Infrastructure Division (EID) Operations staff has access to user log files and audit records described above. General contact information is available to users of the particular resource in the EHI GSS that the user has authorization to access.

- 2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

In the EAD sub-system, access to contact information is available to users with valid active accounts. Access to log files is only available to the Enterprise Administrator.

In the EHS sub-system, there is no content data within the system access. Only configuration and security policy data is stored within the sub-system and only enterprise administrators can access those resources.

Additionally, in the SharePoint portion of the EHS sub-system, users must get approval by SharePoint site administrators (who will be delegated administrative rights by data owners and/or system manager) to access a particular site resource. The access to the hosted data on SharePoint is managed by the data owner and/or subscribing entity. Data owners are responsible for enforcing adequate access controls for the hosted application data that they manage and own.

- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

User's access to all EHI resources will be restricted. Access to contact information stored in the Enterprise Active Directory is available to users with valid active Enterprise Active Directory accounts. Users who have been given access to an application's database content within a security group will have access rights assigned by the SharePoint site administrator. Access to log files is only available to the Enterprise administrators.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

SharePoint users will have restricted access to resources within the SharePoint applications. Firewalls, passwords and authentication requirements will prevent unauthorized access. Users must be included in a security group access list in order to access particular resources. Users are added to site access lists by the SharePoint site administrator. Prior to being given access any EHI SharePoint site resource, users will have to review a specific SharePoint related privacy tutorial and sign the EHI SharePoint Rules of Behavior. All SharePoint users must accept and sign these Rules of Behavior annually thereafter. In addition, all employees and contractors sign general Rules of Behavior before being granted access to Departmental systems, and receive IT Security Awareness Training before being granted access, and annually thereafter.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Yes, contractors are required to sign Non-disclosure agreements (NDAs) and when applicable, disclose any accounts that were created to set up the system or any other accounts that may have been created with elevated privileges to fulfill their duties. Additionally, FAR Regulations

contract clauses concerning following Privacy Act provisions are incorporated into any contracts with companies providing services to these systems.

**6) Do other systems share data or have access to the data in the system? If yes, explain.**

Yes. Other bureau's Active Directory Child Domains authenticate to the EAD Root domain, within the EHI GSS.

The EHI sub-system applications and services, apart from EAD, leverage the Enterprise Active Directory for identification and authentication functionality. Since the EHI will include multiple applications and sub-systems, all of which will be accessible by the subscribing Department of Interior offices and bureau's users, any other bureau system will be able to access the data in a EHI applications or sub-system. However, users' credentials and the access control lists for the content will restrict the data to only those persons who have access to that information.

**7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The System Owner of the EHI.

**8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

No.

**9) How will the data be used by the other agency?**

N/A

**10) Who is responsible for assuring proper use of the data?**

Sharepoint site data owners are responsible for disclosing the accurate classification of their data and accepting the Rules of Behavior prior to subscribing for use of any EHI SharePoint resource. Users are responsible for adhering to the EHI SharePoint system Rules of Behavior that must be signed prior to being granted access to any SharePoint resources. EHS system administrators will be responsible for the maintenance and operational integrity of the system on a daily basis.