



Enterprise Common Security Control System (ECSCS)

Privacy Impact Assessment

Version 3.1

May 2013

Enterprise Common Security Control System Privacy Impact Assessment (PIA)

System Name/Title

The Enterprise Common Security Control System (ECSCS) is an enterprise system comprised of multiple components. All of these components are managed and operated by personnel from the USGS Information Technology Security Operations Team (ITSOT) and Enterprise Computing (eComputing). The purpose of this system is to establish common IT security controls for USGS.

Contact Information

Name: David J. Newman

Title: Privacy Officer

Organization: U.S. Geological Survey/AEI/EI/OIIM

Address: 12201 Sunrise Valley Drive, Mail Stop: 807

City: Reston **State:** VA **Zip code:** 20192

Phone Number: (703) 648-7196

Email Address: djnewman@usgs.gov

System Application /General Information

(1) Does this system contain any information on individuals?

No privacy information about individuals is held in or processed by the ECSCS system. The system is used to provide common security controls across the entire bureau, thus only contains information related to the user and work/office related information, not information about the person specifically.

a. Is this information identifiable to the individual?

No, information is not identifiable to the individual.

b. Is this information about individual members of the public?

No, the information includes only account or logon information for USGS employees or contractors.

c. Is the information about employees?

Yes, there is information about employees stored in the system, but only directly related to their ability to logon to the system or interact with USGS Enterprise systems. No personally identifiable information is available.

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

This PIA covers the Enterprise Common Security Controls System (ECSCS) currently consisting of the following three components:

- IT Security Operations Team Infrastructure
- Enterprise Active Directory
- Enterprise DNS

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

No information protected by the privacy act is held within this system. Therefore no legal authority citation is required.

Data in the System

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

The categories of individuals for this system are comprised of four distinct categories:

- Domain Administrators (<accountname>-**da**) (for eComputing only)
- Certified OU Administrators (<accountname>-**ou**),
- Privileged Users (<accountname>-**pr**), and
- Non-privileged users (<accountname>) including temporary, emergency, and service accounts.

No privacy information exists on this system for any individuals covered on this system.

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

DOI and USGS is the source for the information.

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 primary source of information for this system is taken from an existing internal Lotus Domino database that is synchronized with Microsoft Active Directory objects. The Department of Interior has developed a DOI Access Portal solution as part of the HSPD-12 implementation that is utilized to create Microsoft Active Directory user objects that includes basic user information (UPN, Name, Org Code, Duty Station).

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

The primary Federal Agency providing data for this system is the Department of Interior and U.S. Geological Survey. As part of this system integrated into the Department of Interiors infrastructure (DOI.NET) Microsoft Active Directory Forest that consists of eleven individual Bureaus Active Directory Domains that are integrated into the overall database of MS Directory Services within this system known as the Global Catalog. Currently the USGS maintains their MS Active Directory objects uniquely and independently with exception of mandatory DOI guidelines and Security Technical Implementation Guide (STIG) models. DOI implements a DOI Access Portal solution directly related to HSPD-12 that is utilized to create Microsoft Active Directory user objects.

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

No tribal, state, or local agencies provide data for this system.

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

No data is collected by third party sources. All data is collected by DOI and USGS.

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

Currently, the information collected from the employee is comprised of business data such as employee code, physical location, phone number, and mailing address to create the necessary user account objects.

(3) Accuracy, Timeliness, and Reliability**a. How will data collected from sources other than DOI records are verified for accuracy?**

Currently all data collected is from DOI sources and will be verified before the employee or contractor is provided a system account, each employee is assigned to a specific administrator officer who will verify that these records are verified for accuracy.

b. How will data be checked for completeness?

Currently all data collected is from DOI sources and will be verified before the employee or contractor is provided an account. Each employee is assigned to a specific administrator officer who will check these records for completeness.

c. Is the data current?

Yes, the data is current and updated every 24 hours to synchronize with Lotus Domino database that is currently the authoritative database for the user objects in this system.

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 detail and documented in the User Management Standard Operating Procedure and the AD Naming Standards.

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, the use of data is both relevant and necessary for the designation purposes of this system.

(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, the system will not create previously unavailable data about an individual through aggregation from the information collected.

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

No new data will be placed in the individuals record as a result of aggregation from the information collected.

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

No determinations or new data about employee/public will be placed in the individuals record as a result of aggregation from the information collected.

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

No new data about employee/public will be placed in the individuals record as a result of aggregation from the information collected.

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

Unauthorized access or use is controlled through secure authentication and network firewall controls that provide for internal use only.

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

Yes, unauthorized access or use is controlled through secure authentication and network firewall controls are in place that prevent unauthorized access and provide for internal use only.

(8) How will the data be retrieved?

Data is retrieved after secure authentication with system credentials has been verified and access has been granted through network firewall controls that provide for internal use only.

(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 reports are limited by authorized access only and controlled through secure authentication and network firewall controls. These reports consist of basic business information consisting of (employee code, phone, building, and room number), printers, groups, organization units, and computers that are utilized for authentication and centralized Directory Services purposes. No information such as passwords or privacy information is available through these reports.

(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?

Individuals can decline to provide (employee code, phone, building, room number) that is stored within the Enterprise Active Directory services as requested by their designated administrative officer. This information is available through other internal databases that are not part of this system.

Maintenance and Administrative Controls

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

The Directory Services provided by this system maintains an automated internal database of these objects that is synchronized throughout the system by replication on a scheduled basis. Each site maintains consistent information as the scheduled replication is achieved throughout the system.

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

It is compliant with the general records schedule.

(3) What are the procedures for disposition of the data at the end of the retention period?

The data maintained during this retention period is maintained on designated servers magnetically on disk. The procedures for disposition of the data at the end of the retention period include and overwrite/deletion process of the obsolete data as needed on these disks.

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

The system is using only technologies that are approved and supported by DOI.

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

There is no affect to public/employee privacy due to the system using only technologies that are approved and supported by DOI.

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

Yes, the system will provide the capability to identify, locate, and monitor individuals. The system will identify individuals as they are logged on to this system as part of the event logging that will indicate time and the computer system used to log on. The system can also have the capability to monitor individual activities while logged on the system only when required by security and law enforcement, or as required by DOI officials responsible for ensuring appropriate use of this system.

(7) What kinds of information is collected as a function of the monitoring of individuals?

The information collected as a function of this system are built-in to this system as part of the event logging that will provide specific information on when, where, and who has accessed this system. The information collected provides username, time of log on, logon attempts, computer name and other relevant information on system usage, and security related issues.

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

The controls that will be used to prevent unauthorized monitoring are provided through specific roles assigned on the system to each user. Only designated administrators have the capabilities once authorized by an official requesting monitoring of an individual is requested. All unauthorized monitoring and misuse of privileges for unauthorized monitoring will result in personnel actions resulting in loss of privileges.

(9) Under which Privacy Act Systems of Record notice (SOR) does the system operate?

No PII data in the system.

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

Yes, dependent on the content of records.

Access to Data

(1) Who will have access to the data in the system?

All employees of the Department of the Interior (DOI), U.S. Geological Survey (USGS), and approved cooperators will have access to this system for authentication purposes only. Designated administrators will have management access to the data on this system.

(2) How is access to the data by a user determined?

Access to the data by a user will be determined by their designated role and responsibilities as approved by management.

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

Only designated administrators will have access to modify data on this system. The system is managed and maintained by a designated group of administrators granted access to all data. All other users will have access specific to their area of responsibility and only modify data respective to their office or cost center.

(4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

The controls that will be used to prevent unauthorized use of data are provided through specific roles assigned on the system to each user. Only designated administrators have the capabilities once authorized to manage this system. All unauthorized browsing and misuse of data are controlled through permissions; unauthorized access of data will result in personnel actions resulting in loss of privileges.

(5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?

The system is in a steady state phase with modifications made to enhance the system. Four (4) USGS contractors are involved in the maintenance of the Enterprise Active Directory.

(6) Do other systems share data or have access to the data in the system?

Yes, DOI has been granted access to create new users as part of the HSPD-12 implementation. Currently the Lotus Domino database provides basic user information (employee code, phone, building, room number) that is utilized as the authoritative database for user information and synchronized with the Directory Service for this system. Other systems can utilize this system for authentication purposes.

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

The security and maintenance of this system is provided by a designated group of administrators (domain administrators) and they along with the system owner will protect and ensure the security of the privacy rights for this system.

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

The primary Federal Agency utilizing data for this system is the Department of Interior U.S. Geological Survey. As part of this system we are integrated into the Department of Interiors infrastructure (DOI.NET) that consists of eleven individual bureaus that are integrated into the overall database of Enterprise Active Directory objects within this system known as the Global Catalog. Through separate Active Directory domains each bureau maintains and manages their Microsoft Active Directory objects individually including access.

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

As an integrated system the Microsoft Active Directory objects (user, groups, computers,) will be incorporated into a larger global catalog as part of the native features of this environment. Through separate Active Directory domains each agency maintains and manages their Microsoft Active Directory objects individually including access.

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

The Department of Interior OCIO office through their designated security and administrative staff will ensure proper use of data in the overall system environment. Through separate Active Directory domains each bureau maintains and ensures proper use of their Microsoft Active Directory objects individually including access and use.