




United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

NOV 20 2009

OCIO DIRECTIVE 2010 - 001 007 PH

To: Bureau Chief Information Officers

From: Sanjeev (Sonny) Bhagowalia
Chief Information Officer 

Subject: DOI Access Policy for Bureau/Office Active Directory and Email Systems

Purpose:

This directive establishes the policy to implement and administer the Department of the Interior (DOI) Access Program as required by DOI Personnel Bulletin 09-06, specifically to "Ensure Active Directory (AD) and e-mail system data required by DOI Access are current, accurate, and available."

Background:

DOI Personnel Bulletin 09-06 requires issuance of the Office Chief Information Officer (OCIO) Directives to implement and administer the DOI Access Program in compliance with FIPS 201-1. Personnel Bulletin 09-06 establishes the policy for Bureaus/Offices to implement FIPS 201-1 standard procedures for personal identity verification and PIV credential (DOI Access Card) issuance for DOI employees and contractors. The DOI Access Card is the only authorized PIV credential for these individuals and replaces all existing DOI Bureau/Office issued identity cards.

The standard process for PIV credential issuance is handled through the DOI Access system, which integrates with existing authoritative data sources to establish the identity data required to sponsor employees and contractors for DOI Access Cards with valid active directory credentials.

In order for DOI Access Card to support logical access, the cards must contain the DOI-assigned AD User Principal Name (UPN) and current business email address. This information is required to complete the initial request or Sponsorship, for a DOI Access Card. As outlined in SRFC_20090218_0021 (which was approved by a DOI Systems CAB vote on 3/11/2009), special Organizational Units (OUs) were created in each bureau's Active Directory domain and account creation rights were granted to the DOI Access system to facilitate automated creation of these new accounts.

In addition, this policy is supported by and builds upon OCIO Directive 2006-015.

Scope:

This directive applies to all DOI offices and bureaus except Office of the Inspector General.

Policy:

Creation of New Employee and New Contractor User Accounts in AD (DOI.NET)

Effective November 30, 2009, it is required that all AD accounts for new employees and new contractors are created during the on-boarding and DOI Access Card issuance process through the DOI Access system.

- Use of privileged accounts to create AD user accounts for new employees and contractors is prohibited except for Service or Resource accounts.
- Future enhancements will address the creation of other types of accounts as defined below. Use of privileged accounts to create these types of accounts will be prohibited from that time forward. Guidance is provided in this memo detailing how to create these accounts until such functionality becomes available.
- Deployment of NetIQ Security Manager agents on bureau domain controllers (per 2008 Egov scorecard: Enterprise Infrastructure, Element 5.3) is required to enable monitoring of user account creation. All bureau domain controllers must meet the scorecard requirements by December 28, 2009.

Per Personnel Bulletin 09-06, all user credentials that grant logical access to federally controller information systems must conform to applicable PIV regulations. This memo supersedes information published in the DOI PIV guide published December 2005.

Creation of Designated Service Accounts in Active Directory (DOI.NET)

Effective November 30, 2009, it is required that all new AD accounts that are used as Service accounts adhere to the following requirements.

- The description field for each account must be populated with the word "Service."
- The Manager Name field (under the Organization tab) must be populated with the responsible Federal Employees name.
- The telephone number field must be populated with a responsible Federal Employees telephone number.
- The UPN suffix for each account must be in the form of "@(bureau domain).doi.net"
- Existing service accounts are required to be compliant with this policy no later than December 28, 2009.

Prepare Active Directory for integration with the DOI Access System

Effective November 30, 2009, the following actions must be completed to facilitate the synchronization of data between AD and the DOI Access System:

- AD administrators will populate the business email address, USAccess Enrollment ID (EID), and the FPPS ID into the corresponding AD accounts.
- AD administrators will verify the UPN on DOI Access Cards is identical to the UPN in AD. If they do not match, consideration must be given to determine if there is less impact to modify the data in AD or to update and reload the certificates on the DOI Access Cards.
- AD administrators will identify personnel to assist bureau/office DOI Access Sponsors to identify the correct UPNs for existing employees and contractors.

Prepare Email Systems (e.g.: Lotus Notes, Exchange) for integration with AD

Effective November 30, 2009 the following actions must be completed to facilitate the synchronization of data between email systems and AD:

- Email administrators will create alias in the email system to accept the standard UPN as an alternative email address.
- Email Administrators will populate the email system with the new email addresses generated by DOI Access and stored in the AD Pending OU.
- Email administrators will ensure the verified business email address for all current employees and contractors is entered into the appropriate AD account for those employees and contractors.
- Email administrators will verify the email addresses currently loaded on DOI Access Cards, and when the email is incorrect, provide the correct email address to the bureau DOI Access Lead so the cards can be updated.

Exchange Resource Active Directory Accounts

Microsoft Exchange creates a user account (albeit disabled) for every resource mailbox (calendars, cars, conference rooms, etc.) in Active Directory.

Effective November 30, 2009, it is required that all new Active Directory accounts that are used as Exchange resource mailbox accounts adhere to the following requirements:

- The description field for each Exchange resource account must be populated with "Exchange Resource"

- Existing Exchange resource accounts are required to be compliant with this policy no later than December 28, 2009.

AD Account Definitions

User account: The primary AD account for an employee or contractor. These are not administrative (privileged) accounts, service accounts or Exchange Resource accounts.

Service Account: For the purposes of this document, a service account is any non user account provided as credentials for any service, script, process, task, or automated alternate credential logon.

Exchange Resource Active Directory Account: user accounts created by Microsoft Exchange for resource mailbox use (calendars, cars, conference rooms, etc.) in Active Directory.

Contact:

Questions regarding this directive may be directed to Mr. Tim Quinn, Chief, Enterprise Infrastructure Division at (703) 648-5518 or via email to Timothy.Quinn@ios.doi.gov.

cc: Bureau Deputy Chief Information Officers