

Summary: Active Directory Misconfigurations Place DOI Mission Critical Systems at Serious Risk of Compromise

Report Date: September 03, 2026

Report Number: 2024-CTD-025

This report presents the results of our inspection of the U.S. Department of the Interior's (DOI's) Active Directory (AD) configuration and management practices. Our objective was to determine whether DOI's AD configurations were adequate to protect mission critical systems and data. We focused our review on select AD domains at five bureaus: Bureau of Land Management, Bureau of Reclamation, Bureau of Trust Funds Administration, the National Park Service, and the U.S. Geological Survey. To accomplish our objective, we collected data from September 3, 2024, to February 6, 2025. We reported our initial findings to the bureaus and the Office of the Chief Information Officer (OCIO) between May 7, 2025, and July 9, 2025.

We found that four of the five DOI bureaus that we reviewed did not ensure that their AD domains were configured to reduce the risk of compromise to DOI systems. Specifically, we found passwords were not stored in encrypted form, sensitive information was accessible DOI-wide, standard users were granted excessive privileges, inactive accounts were not disabled when required, and accounts were configured with inherent authentication weakness. The exploitation of any of these vulnerabilities could result in severe adverse effects on DOI operations and, in combination, could greatly increase the effect of a successful compromise.

Although the data we analyzed were collected prior to the consolidation of bureau and office IT staff and functions under OCIO, at the request of OCIO, we are directing all recommendations to OCIO due to the ongoing consolidation efforts. We make eight recommendations to strengthen DOI's AD configuration and management processes across all its bureau AD domains and to reduce the risk of loss of sensitive data and disruption to mission operations.

OCIO concurred with all eight recommendations and implemented seven of the recommendations after responding to our draft report. Therefore, we consider seven recommendations closed and one recommendation resolved. With respect to the resolved recommendation, OCIO's original target implementation date was July 15, 2026. After it responded to our draft report, OCIO revised its target implementation date to January 29, 2027. We will track implementation of the recommendation.

This is a summary of a report we provided to OCIO.

