



# At a Glance

## Why We Did This Review

We sought to determine to what extent the U.S. Environmental Protection Agency (EPA) implemented a management control structure for its directory service infrastructure. We also sought to determine what steps EPA took to identify and disable user accounts that are no longer needed.

A directory service provides a centralized location to store information about the users, computers, and other equipment on a network and provides integrated services that are used to manage network users, services, and devices. EPA uses a commercial off-the-shelf product for its directory service system (DSS). EPA implements this system using multiple servers placed in various locations on its network to provide enterprise-wide authentication and authorization.

## This report addresses the following EPA Goal or Cross-Cutting Strategy:

- *Strengthening EPA's Workforce and Capabilities*

For further information, contact our Office of Congressional and Public Affairs at (202) 566-2391.

## ***EPA Should Improve Management Practices and Security Controls for Its Network Directory Service System and Related Servers***

### What We Found

The Office of Environmental Information (OEI) is not managing key system management documentation, system administration functions, the granting and monitoring of privileged accounts, and the application of environmental and physical security controls associated with its DSS. OEI is not keeping management documentation associated with the DSS current and complete, and does not have an effective process for maintaining this documentation. Further, OEI is not performing user account administration practices for the DSS, and does not have a management oversight process to ensure that the regions and program offices are managing their delegated responsibilities in accordance with Agency and federal requirements. The Office of Administration and Resources Management's (OARM's) Human Resources and Contractor Management systems and processes are not linked to the user account management function. OEI is also not managing the delegation of DSS logging and monitoring processes. Lastly, OEI is not ensuring that environmental and physical security controls are applied to protect the authentication and authorization servers.

### Recommendations and Agency Corrective Actions

We recommended that OEI and OARM management undertake a number of corrective actions to improve its management of, and correct specific deficiencies associated with, the Agency's DSS.

OEI and OARM management concurred with all recommendations, other than two associated with environmental and physical security controls, and completed or agreed to take corrective actions to address the recommendations with which they concurred.

OEI indicated that the particular physical and environmental controls are not its responsibility. We disagree. The DSS Authentication and Authorization servers belong to OEI, and OEI is responsible for managing this equipment. Therefore, OEI needs to ensure that these controls are in place.

Due to the sensitive nature of the report's security findings, the full report is not available to the public.