24-P-0005
October 31, 2023

At a Glance

The EPA Needs to Better Implement Internal Access Control Procedures for Its Integrated Risk Information System Database

Why We Did This Audit

To accomplish this objective:

The U.S. Environmental Protection Agency Office of Inspector General conducted this audit to determine whether the EPA's Integrated Risk Information System database adheres to federal and Agency access control requirements. The Integrated Risk Information System Program is a chemical evaluation program under the Office of Research and Development and is a critical component of the EPA's capacity to support scientifically sound environmental regulations and policies. The program supports the EPA's mission to protect human health and the environment by identifying and characterizing the health hazards of chemicals found in the environment. The Office of Research and Development operated with a $574.4 million budget in fiscal year 2023 with an estimated $11.3 million allocated to the program. Agency personnel estimated $127,000 of the program's budget was used for its database application.

This audit supports EPA mission-related efforts:

- *Compliance with the law.*
- *Operating efficiently and effectively.*

This audit addresses this top EPA management challenge:

- *Protecting EPA systems and other critical infrastructure against cyberthreats.*

Address inquiries to our public affairs office at (202) 566-2391 or OIG.PublicAffairs@epa.gov.

List of OIG reports.

What We Found

We found that information technology access management for the EPA's Integrated Risk Information System database did not adhere to federal and Agency IT access control requirements. Specifically, our analysis identified significant deficiencies including the following:

- Sixty-four percent of IRIS Database Application general user accounts had access to the application without a legitimate business need, allowing two users to remain active for eight months after they separated from the Agency.
- On the application's database server, privileged user accounts remained in an active status without adhering to access control requirements, resulting in the use of a generic shared administrator account for over 11 years, an active account for an employee separated from the Agency for over two years, and a privileged account with unnecessary elevated privileges.
- The EPA failed to implement password configurations for IRIS database server accounts, which caused inactive accounts to remain in an active status for an unlimited time frame, use the same password an unlimited amount of time, and reuse a password sooner than allowed.
- The Agency ran the database without being included or identified in a system security plan that would ensure that the system's security met federal standards.

These issues occurred because the EPA did not perform regular reviews or monitor privileged or application user accounts for the IRIS Database Application. Additionally, password settings for the IRIS database server were implemented at the time the database was created with no monitoring in place to ensure ongoing compliance as requirements changed. Finally, Agency personnel assumed IRIS was included in the National Computer Center's Hosting System's system security plan, but no mention of the application is documented in that plan.

Without enforcing established access control requirements, the EPA puts the chemical data, which IRIS users rely upon to inform scientifically sound environmental regulations and policies, at risk of unauthorized changes.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Research and Development develop processes and assign responsibilities for the approval, review, and monitoring of user access of the IRIS Database Application. Additionally, we recommend that the assistant administrator for Mission Support implement and document password configurations for the IRIS database server to comply with federal and Agency requirements. We also recommend that the Office of Research and Development work with the Office of Mission Support to ensure security control implementation is documented for the IRIS Database Application. The Agency agreed with our recommendations, completed corrective actions for one recommendation, and provided acceptable planned corrective actions with estimated milestone dates for the remaining recommendations. We consider the recommendations resolved with corrective actions pending.