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

October 31, 2023 | Report No. 24-P-0005

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

Report Contributors

Tertia Allen
Yoon An
LaSharn Barnes
LaVonda Harris-Claggett
Eric Jackson Jr.
Alonzo Munyeneh
Sabrena Richardson
Jeremy Sigel

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
GSS	General Support System
IRIS	Integrated Risk Information System
IT	Information Technology
NHS	National Computer Center Hosting System
OIG	Office of Inspector General
OMS	Office of Mission Support
ORD	Office of Research and Development

Key Definitions

Please see Appendix A for key definitions.

Cover Image

The EPA lacks consistent implementation of required information technology access controls for its Integrated Risk Information System. (EPA OIG image)

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.

OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

October 31, 2023

MEMORANDUM

SUBJECT: The EPA Needs to Better Implement Internal Access Control Procedures for Its Integrated Risk Information System Database
Report No. 24-P-0005

FROM: Sean W. O'Donnell, Inspector General

TO: Kimberly Patrick, Principal Deputy Assistant Administrator
Office of Mission Support

Dr. Chris Frey, Assistant Administrator and EPA Science Advisor
Office of Research and Development

This is our report on the subject audit conducted by the U.S. Environmental Protection Agency Office of Inspector General. The project number for this audit was OA-FY22-0071. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Mission Support and the Office of Research and Development are responsible for the issues discussed in this report.

In accordance with EPA Manual 2750, your offices provided acceptable planned corrective actions and estimated milestone dates in response to OIG recommendations. All recommendations are resolved, and no final response to this report is required. If you submit a response, however, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epaoig.gov.

Table of Contents

Chapters

Appendixes

Chapter 1
Introduction

Purpose

The U.S. Environmental Protection Agency Office of Inspector General initiated this audit to determine whether the EPA's Integrated Risk Information System database adheres to federal and Agency access control requirements.

Top management challenge addressed

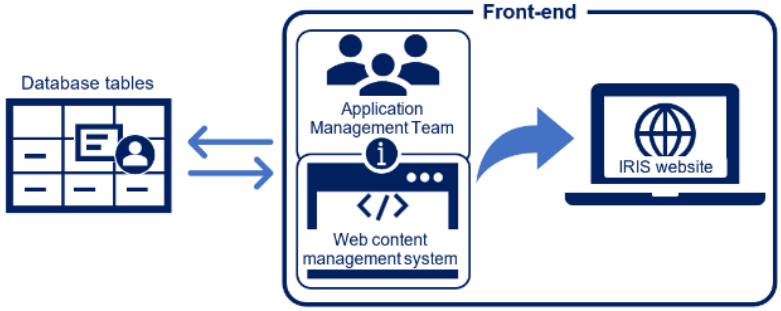
This audit addresses the following top management challenge for the Agency, as identified in the OIG's *U.S. Environmental Protection Agency Fiscal Year 2023 Top Management Challenges* report, issued October 28, 2022:

- Protecting EPA systems and other critical infrastructure against cyberthreats.

Background

The EPA's Integrated Risk Information System Program is a chemical evaluation program under the Office of Research and Development that the Agency considers to be a critical component of its capacity to support scientifically sound environmental regulations and policies. The IRIS 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 IRIS database presents toxicity information on more than 540 chemicals to the public through its website.

The various information technology environments that make up the IRIS database's operating structure include the database tables, which store and manage application user data and configurations. Additionally, the front-end, which is the part of an information system that is directly accessed and interacted by the ORD's Application Management Team, interfaces to the database tables. The IRIS database's web content management system is used to link and release IRIS content on its website.



The application piece of the IRIS database, referred to as the IRIS Database Application and does not include general users of its public website, consists of two modules: (1) a data entry module to create and update chemical landing webpages that provide the final IRIS assessments and (2) a tracking module to update the schedule of chemical assessments under development. The focus of our audit was on access to these modules of the IRIS Database Application, its underlying database server, and its web

content management system administrators, and did not include review of scientific content, assessment process, or evaluation of the scientific conclusions presented by the IRIS Program.

General Support System
Interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Major Application
An application that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Minor Applications
An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

During the pertinent time frame of our audit, the Agency's *Information Security – Access Control Procedure*, CIO Directive 2150-P-01.2, required owners of all EPA information and information systems to comply with the user access controls, including review of active user accounts, in accordance with the National Institute of Standards and Technology Special Publication 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. Similarly, the Agency's CIO Directive *Information Security—Identification and Authentication Procedure*, CIO Directive 2120-P-07.2, provided requirements for user password settings.[1]

The IRIS Database Application was implemented in 2001, according to ORD personnel,[2] and is hosted within the Agency's National Computer Center in Research Triangle Park, North Carolina. While the IRIS Program is located within the ORD, its database development is performed by the ORD and the EPA's Office of Mission Support, or the OMS, contractors. EPA personnel who interact with the IRIS database includes ORD database and application developers, known as the ORD's Application Management Team; OMS server administrators; and an OMS database administrator. The OMS provides operational support for the underlying infrastructure running the servers on which the IRIS Database Application resides. This support consists of managing the operating system; deploying patches, which is the distribution and application of updates to software; and implementing updates the ORD's Application Management Team sent in production, but not running the application itself.

ORD personnel, including the Application Management Team and the IRIS application owner, manage access to the IRIS Database Application. Requests for new accounts would be routed to the Application

[1] Version 2 (2150-P-01.2) of the *Access Control Procedure* was in effect during the primary time period of this audit. On June 8, 2023, version 3 (2150-P-01.3) was issued to implement the National Institute of Standards and Technology Special Publication 800-53 Revision 5 requirements. Similarly, version 2 (2120-P-07.2) of the *Identification and Authentication Procedure* was in effect during the time period of this audit; on January 1, 2023, version 3 (2120-P-07.3) was issued to update for the National Institute of Standards and Technology requirements. Accordingly, this report references the prior versions of both procedures.
[2] As shown in Chapter 4, a system security plan that would support this implementation date was not documented for the IRIS database due to the Agency's assumption that it was included as a minor application under the National Computer Center Hosting System general support system's security plan.

Management Team, who creates the accounts. However, ORD personnel stated that they have not received requests for IRIS access in several years. The ORD Application Management Team only uses these accounts to display chemical managers' names with their associated public draft assessment on the IRIS website. Only the ORD Application Management Team has direct access to the IRIS Database Application.

System security plan
A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

The ORD classifies its IRIS Database Application as a minor application under the National Computer Center Hosting System general support system, or NHS GSS, owned by OMS's Enterprise Hosting Division. The NHS supports large-scale data processing and provides a national data repository for Agency environmental and administrative systems. NHS also provides dedicated, shared, and virtualized computing resources running multiple various operating systems. While all EPA information systems are required to follow Agency IT procedures, a system security plan detailing the controls planned or implemented to meet security control requirements is required for the GSS and major applications. Since most of the security controls are provided by the GSS, security controls specific to the minor application, including access controls, should be documented as part of the GSS system security plan. Additionally, the National Institute of Standards and Technology's Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, issued February 2006, states that minor applications that are not connected to a major application should be briefly described in their general support system plans.

Responsible Offices

The IRIS Program, which has an estimated fiscal year 2023 budget of $11.3 million and owns the IRIS Database Application, is located within the EPA's Center for Public Health and Environmental Assessment in the ORD. The ORD is responsible for providing the data, tools, and information that form the scientific foundation the Agency relies on to fulfill its mission to protect the environment and safeguard public health. The Center for Public Health and Environmental Assessment is responsible for providing the science needed to support assessments and policies to protect human health and ecological integrity. The ORD's Application Management Team is responsible for the access management and administration of the IRIS Database Application, which has an estimated fiscal year 2023 budget of $127,000.

The OMS leads the EPA's information management and information technology programs. Within the OMS, the Office of Information Technology Operations implements and manages the Agency's information technology services and solutions, including computers, servers, software, and networks. Its Enterprise Hosting Division personnel at the National Computer Center provide system administration for the NHS GSS, under which the IRIS Database Application is a minor application. The Enterprise Hosting Division also administers the production server on which the IRIS Database Application resides.

Scope and Methodology

We conducted this performance audit from February 2022 to April 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We assessed the internal controls necessary to satisfy our audit objectives.[3] In particular, we assessed internal control components—as outlined in the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*—significant to our audit objectives. Any internal control deficiencies we found are discussed in this report. Because our audit was limited to the internal control components deemed significant to our audit objective, it may not have disclosed all internal control deficiencies that may have existed at the time of the audit.

We gained an understanding of the IRIS Database Application's IT access control processes through interviews with the ORD's Application Management Team and the OMS's database server administration personnel. We requested and analyzed documentation and system-generated evidence to corroborate statements from the ORD and the OMS and identified vulnerabilities or IT access security control weaknesses. This evidence consisted of system security documentation as well as database tables containing IRIS Database Application user listings, system and administration accounts, and password configurations for the database server. To verify system data, we performed virtual walkthroughs with IRIS IT operations personnel. The scope of our audit was limited to IT access for the IRIS Database Application and did not include review of scientific content, assessment process, or evaluation of the scientific conclusions presented by the IRIS Program.

Prior Reports

OIG Report No. 21-E-0226, *EPA's Emergency Response Systems at Risk of Having Inadequate Security Controls*, issued September 13, 2021, evaluated whether the system security plans in the ORD, among other offices, were developed and updated in accordance with the National Institute of Standards and Technology standards and guidance. We recommended that the assistant administrator for Research and Development "develop and implement a process to list and describe all minor applications in the appropriate system security plan." The ORD concurred with this recommendation and provided acceptable corrective actions that were completed by May 4, 2022.

[3] An entity designs, implements, and operates internal controls to achieve its objectives related to operations, reporting, and compliance. The U.S. Government Accountability Office sets internal control standards for federal entities in GAO-14-704G, *Standards for Internal Control in the Federal Government* (also known as the "Green Book"), issued September 10, 2014.

Chapter 2
IRIS Database Application's IT Environments Includes Unused, Duplicate, Shared, and Generic Accounts

The EPA's account management for the IRIS Database Application failed to adhere to federal and Agency IT access control requirements. Among the IRIS Database Application's 163 user accounts, we found that the EPA did not manage and monitor privilege and general user accounts with active access to the IRIS Database Application, resulting in 104 general user accounts (64 percent) with active access to the application without having a business or mission need. Specifically, we found two privilege user accounts in an active status using a generic shared administrator account and one account for an employee who separated from the Agency. Additionally, for the database server hosting IRIS, we found shared and open accounts with elevated privileges that allows unauthorized updates or the ability to lock data. Finally, for IRIS's web content management system responsible for publishing and editing content on IRIS's chemical risk assessment website, two of the five administrators (40 percent) had more than one account with administrator privileges.

Specifically, for the IRIS Database Application general user accounts, we found that:

- 104 of 163 (64 percent) IRIS Database Application user accounts did not require access to the IRIS Database Application for their business or mission functions as confirmed by ORD personnel.

- Two IRIS Database Application user accounts remained in an active status for eight months after the employees assigned to these accounts separated from the Agency.

- An IRIS Database Application user account was created during this audit without formal or documented approval.

Following a March 2022 inquiry from us on the identified findings, the ORD reviewed, disabled, and locked most of these accounts. However, as of August 2022, the ORD still had 18 active IRIS Database Application user accounts that required review to determine whether those users need access to the IRIS Database Application.

Additionally, in the database server hosting IRIS we found that:

- The Agency did not restrict the use of a generic administrator account, which was active for more than 11 years. Lack of restrictions such as this exposes the Agency to an internal threat of a bad actor using the account to perform unauthorized transactions without accountability.

- The Agency allowed the account for an administrator responsible for monitoring IRIS Database Application user IT access and account management to remain active for more than two years after the employee retired from the Agency. Leaving a separated employee's account active, especially an administrator account, exposes the database to internal threats such as the account being used for unauthorized activity.

- An active IRIS Database administrator account to which multiple people have access and should be reviewed for business function and restricted accordingly, provided users with unnecessary elevated account privileges that could allow them to make changes to the IRIS Database Application tables. While the OMS is aware of the account's assigned roles, it was unaware of who uses the account and why.

- The IRIS Database Application's Object Owner Account was not disabled and locked when it was not performing installation and maintenance actions. This account is the user who creates database objects such as tables and necessitates special precautions against unauthorized access when not in use since the account owns all objects of the application. In addition to its elevated privileges for database installation and maintenance, this account is designed for infrequent use, meaning that unauthorized access to the account could go undetected.

Finally, in its web content management system, we found that the Agency did not disable and lock two duplicate administrator accounts. These accounts allow users to edit, publish, and delete content on the IRIS website.

The Agency's *Information Security – Access Control Procedure*, CIO Directive 2150-P-01.2, required owners of EPA-operated systems to "review users' activities to enforce use of information system access controls." Additionally, CIO Directive 2150-P-01.2 requires immediately disabling all accounts that are not accessed by the user for more than 30 days and when a user is no longer associated with the EPA. In addition, the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations,* requires agencies to "[re]view accounts for compliance with account management requirements," as well as to disable accounts in accordance with organizational policy and procedures. Additionally, CIO Directive 2150-P-01.2 stated that the Agency's procedures "cover all EPA information and information systems" and it does not exempt minor applications from its requirements.

These oversights occurred because the EPA failed to conduct periodic reviews of whether users were granted access to the IRIS Database Application's IT environments in accordance with federal and Agency IT access control requirements. This was exacerbated by the lack of monitoring of privileged user accounts and activity to identify suspicious activity and mitigate the associated risks. The ORD stated

that the application owner who performed the account reviews retired in January 2018, and that the ORD no longer reviewed these accounts because it transitioned away from using the IRIS Database Application to track assessment milestones and instead uses IRIS Program Outlook documents, which are updated three times a year. IRIS Program Outlook documents track the status of assessments and forecast future milestones, such as finalizing chemical assessment plans, public comment deadlines, and external peer reviews. However, the IRIS Database Application is still used to display milestone information on the IRIS website and the ORD Application Management Team updates the assessment milestones in the IRIS Database Application when necessary.

Without enforcing federal and Agency access control requirements, the EPA risks exposing its chemical risk data, which IRIS users rely upon to inform environmental regulations and policies, to unauthorized access and changes. This could allow a threat actor to perform unauthorized system changes that may negatively affect the operation of the Agency system and integrity of its data. Because the EPA does not review these accounts or monitor their activity, malicious acts could go undetected.

Recommendations

We recommend that the assistant administrator for Research and Development:

1. Develop a process and assign responsibility for periodic review of application user information technology access for the Integrated Risk Information System database and perform the necessary updates to adhere to federal and Agency information technology access controls requirements including identifying and deactivating any unused accounts.

2. Develop a process and assign responsibility for application user information technology access approval to the Integrated Risk Information System database.

3. Instruct staff responsible for Integrated Risk Information System account management of the federal and Agency information technology access control requirements related to access approval, review, monitoring, and removal.

4. Discontinue use of IRIS Database Application accounts for database administration activities without a business justification or develop a process to track privileged user activity on these accounts.

Agency Response and OIG Assessment

The ORD agreed with our four recommendations and provided acceptable planned corrective actions and estimated milestone dates. We consider these recommendations resolved with corrective action pending.

For Recommendations 1 and 2, the ORD stated that it would develop and implement a user account management procedure for internal access to the database that would include periodic review of

application user access. Additionally, this procedure would include a process for identifying, approving, and deactivating unused accounts in accordance with federal and Agency access control requirements.

For Recommendation 3, the ORD stated that it would add the ORD Application Management Team to the ORD Significant Information Security Responsibility list, which will require it to complete five additional security related training credits managed by the ORD information security officer, who certifies completion annually.

For Recommendation 4, the ORD stated that it is in the process of reviewing and disabling IRIS Database Application user accounts and will include a process to track privileged user activity on IRIS Database Application accounts for database administration in the user account management procedure.

Appendix B contains the Agency's response to the draft report.

Chapter 3
IRIS Database Server Password Configurations Do Not Comply with Agency Requirements

The EPA did not implement compliant password configurations to secure the IRIS database, which allowed for inactive accounts to remain active for an unlimited time, unlimited use of the same password, and password reuse sooner than required, as well as jeopardized the confidentiality, reliability, and integrity of IRIS's chemical risk data, as shown in Table 1.

Inactive account time
The number of days an inactive account can remain active.

Password lifetime
The number of days a password remains valid.

Password reuse maximum
The number of different passwords that must be used before the user is allowed to reuse a password.

Specifically, we found that:

- Inactive account time password settings for the default and system database server profiles allow inactive accounts to remain active for an unlimited time instead of adhering to the 30-day Agency requirement.
- Password lifetime settings for the default database server profile allows 90 days of use and the system database server profiles allows unlimited use of the same password instead of adhering to the 60-day Agency requirement.
- Password reuse maximum settings allow passwords to be reused sooner than required, specifically after five password changes instead of 24, or four years, as required in Agency procedures.

Table 1: Noncompliant password settings implemented on the IRIS database server

Password Setting	Associated IRIS database server profile	Current Setting	Directive Requirement	Directive
Inactive Account Time	Default	Unlimited	30 days	CIO-2150-p-01.2
Password Lifetime	Default	90 days	60 days	CIO-2120-p-07.2
Password Reuse Max	Default	Five cycles	24 cycles	CIO-2120-p-07.2
Inactive Account Time	System	Unlimited	30 days	CIO-2150-p-01.2
Password Lifetime	System	Unlimited	60 days	CIO-2120-p-07.2

Source: OIG analysis of IRIS database server configurations. (EPA OIG table)

CIO Directive 2150-P-01.2, *Information Security – Access Control Procedure*, required deactivating accounts for EPA-operated systems after 30 days of nonuse. CIO Directive 2120-P-07.2, *Information Security – Identification and Authentication Procedure*, restricted password lifetime for all information systems to 60 days and the reuse of passwords within 24 cycles or four years. Additionally, CIO Directive 2150-P-01.2 required owners of all information systems to review system accounts and access at least monthly to ensure that only the appropriate levels of access are allowed.[4]

These instances occurred because the EPA did not monitor password settings to ensure compliance with Agency requirements. Specifically, the OMS implemented these settings at the time the database was created and did not update the database's password settings as policy requirements changed. The Office of Information Technology Operations reviews compliance with issued policy by validating the database's password settings against the policy in place during the annual review of system security plans. According to Office of Information Technology Operations personnel, updates and changes resulting from this review are disseminated to the technical teams; however, no updates were communicated or tracked as part of this review.

Without controls in place to monitor and verify compliance with Agency requirements, the EPA hinders its ability to enforce its password policies to protect the confidentiality, reliability, and integrity of IRIS's chemical risk data. Additionally, weak password settings could be used to exploit weaknesses in the IRIS database and leave them vulnerable to emerging threats.

Recommendations

We recommend that the assistant administrator for Mission Support:

5. Configure password settings to comply with Agency access control requirements for the password expiration, password reuse maximum, and inactive account time password settings.

6. Document the Integrated Risk Information System database's security controls, including password configuration settings, in a system security plan and work with the Office of Information Technology Operations to confirm those settings are reviewed as part of its annual security plan review process.

Agency Response and OIG Assessment

The OMS agreed with our recommendations; completed corrective actions for Recommendation 5; and provided acceptable planned corrective actions and estimated milestone dates for Recommendation 6, which we consider resolved with corrective action pending.

[4] Version 3 of CIO Directive 2150-P-01 now requires reviewing accounts for compliance every 60 days, and the time frame for disabling accounts afer periods of inactivity was also changed based on whether the information system is classified as a low, moderate, or high security system. The applicable requirements in Version 3 of CIO Directive 2120-P-07 did not change.

The OMS stated that a compensating control, in the form of a daily automated tracking process, is in place for the inactive account time password settings for the default and system database server profiles. This daily process checks for accounts past 30 days of inactivity and locks those accounts. This is done to prevent the database from locking accounts critical to the operations of the application which has the potential to negatively impact its ability to support Agency missions. The OMS provided acceptable corrective actions for Recommendation 5, which it completed on August 12, 2022. We consider this recommendation complete.

For Recommendation 6, the OMS stated that it would document the IRIS database's internal security controls, including password configuration settings, in a system security plan and work with the Office of Information Technology Operations to confirm those settings are reviewed as part of its annual security plan review process. Recommendation 6 is resolved with planned corrective action pending.

The Agency's response to the draft report is in Appendix B.

Chapter 4
IRIS Database Application Lacks Required System Documentation for Operating in the Agency's Production Environment

The EPA operated the IRIS Database Application in the production environment without the required system security documentation. Specifically, it was not included in a system security plan. Federal standards require all information systems to be covered by a system security plan. While the EPA documented a system security plan for the NHS GSS, the plan does not identify the IRIS Database Application as its minor application or address IRIS's inherited or system level security controls. This oversight can result noncompliance issues, such as the findings detailed in Chapter 3, in that, validating a system's compliance with public policy would not occur without a system security plan to review them against.

Production environment
Where the latest versions of software, products, or updates are pushed live to the intended users. This is the environment where the end user can see, experience, and interact with the new product.

The National Institute of Standards and Technology's Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, issued February 2006, states that:

> Specific system security plans for minor applications are not required because the security controls for those applications are typically provided by the general support system or major application in which they operate. In those cases where the minor application is not connected to a major application or general support system, the minor application should be briefly described in a general support system plan that has either a common physical location or is supported by the same organization.

This oversight occurred because ORD and National Computer Center personnel wrongly assumed IRIS was incorporated in the NHS SSP; however, our audit found no specific mention of the IRIS Database Application in the system security plan. While the NHS system security plan was created in 2010, the IRIS Database Application has been in operation since 2001, according to ORD personnel. It should be part of the NHS plan.

Without the required system documentation, the EPA cannot ensure that the security of its systems meet federal standards to operate in a production environment. The system security plan is designed to improve protection of information system resources and prevent noncompliance issues such as the password findings detailed in Chapter 3.

Recommendation

We recommend that the assistant administrator for Research and Development:

7. Work with the Office of Mission Support to incorporate the Integrated Risk Information System database into the National Computer Center's Hosting System's security plan.

Agency Response and OIG Assessment

The ORD agreed with Recommendation 7 and provided acceptable planned corrective actions. The ORD stated that it would work with the OMS to obtain an Authorization to Use approval, the management decision given to authorize the use of an information system, via the Application Characterization Document review process, which should result in the incorporation of the IRIS database into the National Computer Center's Hosting System's security plan. The Application Characterization Document contains relevant application description information to include in the security plan. We consider this recommendation resolved with corrective action pending.

Status of Recommendations

Rec. No.	Page No.	Recommendation	Status*	Action Official	Planned Completion Date
1	7	Develop a process and assign responsibility for periodic review of application user information technology access for the Integrated Risk Information System database and perform the necessary updates to adhere to federal and Agency information technology access controls requirements including identifying and deactivating any unused accounts.	R	Assistant Administrator for Research and Development	12/31/24
2	7	Develop a process and assign responsibility for application user information technology access approval to the Integrated Risk Information System database.	R	Assistant Administrator for Research and Development	12/31/24
3	7	Instruct staff responsible for Integrated Risk Information System account management of the federal and Agency information technology access control requirements related to access approval, review, monitoring, and removal.	R	Assistant Administrator for Research and Development	12/31/24
4	7	Discontinue use of IRIS Database Application accounts for database administration activities without a business justification or develop a process to track privileged user activity on these accounts.	R	Assistant Administrator for Research and Development	12/30/24
5	10	Configure password settings to comply with Agency access control requirements for the password expiration, password reuse maximum, and inactive account time password settings.	C	Assistant Administrator for Mission Support	
6	10	Document the Integrated Risk Information System database's security controls, including password configuration settings, in a system security plan and work with the Office of Information Technology Operations to confirm those settings are reviewed as part of its annual security plan review process.	R	Assistant Administrator for Mission Support	12/30/24
7	13	Work with the Office of Mission Support to incorporate the Integrated Risk Information System database into the National Computer Center's Hosting System's security plan.	R	Assistant Administrator for Research and Development	12/30/25

* C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

Key Definitions

General Support System: Interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Major Application: An application that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Minor Applications: An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Production environment: The environment where the latest versions of software, products, or updates are pushed live to the intended users. The end user can see, experience, and interact with the new product.

System Security Plan: A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Agency's Response to the Draft Report

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

September 19, 2023

OFFICE OF
RESEARCH AND DEVELOPMENT

MEMORANDUM

SUBJECT: Response to Office of Inspector General (OIG) Draft Report, "The EPA Needs to Better Implement Access Control Procedures for Its Integrated Risk Information System" (Report No. OA-FY22-0071, dated August 15, 2023)

FROM: H. Christopher Frey
Assistant Administrator and EPA Science Advisor
Office of Research and Development

H. CHRISTOPHER FREY
Digitally signed by H. CHRISTOPHER FREY
Date: 2023.09.19 13:54:55 -04'00'

Vaughn Noga
Chief Information Officer and Deputy Assistant Administrator for Environmental Information
Office of Mission Support

VAUGHN NOGA
Digitally signed by VAUGHN NOGA
Date: 2023.09.21 08:39:27 -04'00'

TO: Sean W. O'Donnell
Inspector General
Office of Inspector General

The EPA's Office of Research and Development (ORD) and Office of Mission Support (OMS) appreciates the opportunity to review and comment on the OIG's Draft Report titled "*The EPA Needs to Better Implement Access Control Procedures for Its Integrated Risk Information System*" (Report No. OA-FY22-0071). EPA's Program for the Integrated Risk Information System (IRIS) develops scientific assessments that provide an important source of toxicity information used by EPA, state and local health agencies, other federal agencies, and international health organizations. These assessments, in the form of reports, associated materials, and general information, are made available to the public via several webpages and applications commonly referred to as the IRIS database.

The IRIS database serves as an information technology platform for EPA to conveniently share Agency IRIS assessment related information. IRIS assessments are separately and independently developed, reviewed, and completed in the form of written EPA documentation.

This OIG review and associated recommendations are focused on the internal information security procedures for accessing the IRIS database (i.e., internal access to the technology application). The internal access control procedures highlighted in this draft report are not related

to, and have no impact on, the scientific activities, assessment development and review, assessment content, and communications generated by the IRIS Program. In light of the OIG recommendations in the draft report, EPA understands that improvements can be made to underlying security procedures associated with internal access controls to the IRIS database. EPA is committed to ensuring the information technology aspect of the IRIS database remains secure. EPA intends to take steps indicated by the OIG to improve the security procedures associated with the internal controls of the IRIS database and to ensure that best practices are maintained and followed.
Immediately below are EPA's responses to the OIG's recommendations.

Recommendation 1: Develop a process and assign responsibility for periodic review of application user information technology access for the Integrated Risk Information System database and perform the necessary updates to adhere to federal and Agency information technology access controls requirements including identifying and deactivating any unused accounts.

ORD Response: ORD concurs with this recommendation and proposes the following corrective action and completion date.

Corrective Action 1: ORD will develop and implement a User Account Management Procedure for internal access to the database. This procedure will include the following:

- A process, including assigned responsibility, for periodic review of application user technology access.
- A process for identifying and deactivating unused accounts in accordance with federal and Agency information technology access control requirements.
- A process, including assigned responsibility, for application user information technology access approval.
- Instructions for staff responsible for IRIS account management of the federal and Agency information technology access control requirements related to access approval, review, monitoring, and removal.
- A process to track privileged user activity on IRIS Database Application accounts for database administration.

Planned Completion Date: December 31, 2024

Recommendation 2: Develop a process and assign responsibility for application user information technology access approval to the Integrated Risk Information System database.

ORD Response: ORD concurs with this recommendation and proposes the following corrective action and completion date.

Corrective Action 2: ORD will develop and implement a User Account Management Procedure for internal access to the database. As outlined in the response to recommendation one, this procedure will include a process for assigned responsibility for application user information technology access approval.

Planned Completion Date: December 31, 2024

Recommendation 3: Instruct staff responsible for Integrated Risk Information System account management of the federal and Agency information technology access control requirements related to access approval, review, monitoring, and removal.

ORD Response: ORD concurs with this recommendation and proposes the following corrective actions and corresponding completion dates.

Corrective Action 3a: The ORD Information Security Officer (ISO) will add the Application Management Team to the ORD Significant Information Security Responsibility (SISR) list. Individuals who are designated with this requirement must complete five additional security related training Continuing Professional Education (CPE) credits in addition to completing the agency's Annual Information Security and Privacy (ISPAT) course. The security training is managed by the ORD ISO, who certifies ORD completion annually to the Office of Information Security and Privacy (OISP).

Planned Completion Date: December 31, 2023

Corrective Action 3b: ORD will develop and implement a User Account Management Procedure for internal access to the database. As outlined in the response to recommendation one, this procedure will include instructions for staff responsible for IRIS database account management of the federal and Agency information technology access control requirements related to access approval, review, monitoring, and removal.

Planned Completion Date: December 31, 2024

Recommendation 4: Discontinue use of IRIS Database Application accounts for database administration activities without a business justification or develop a process to track privileged user activity on these accounts.

ORD Response: ORD concurs with this recommendation and proposes the following corrective actions and completion dates.

Corrective Action 4a: The Application Management Team is in the process of reviewing and disabling, as appropriate, the IRIS Database Application user accounts that were previously used to display the point(s) of contact on the various assessments in development.

Planned Completion Date: December 31, 2023

Corrective Action 4b: Additionally, ORD will develop and implement a User Account Management Procedure for internal access to the database. As outlined in the response to recommendation one, this procedure will include a process to track privileged user activity on IRIS Database Application accounts for database administration.

Planned Completion Date: December 30, 2024

Recommendation 5: Configure password settings to comply with Agency access control requirements for the password expiration, password reuse maximum, and inactive account time password settings.

OMS Response: OMS agrees with this recommendation for account settings that do not have compensating controls and has resolved this issue. OITO has implemented updates to the daily monitoring script to verify Password Lifetime, Password Reuse Max settings are complying with policy. This script notifies appropriate personnel of non-compliant settings and updates are implemented during weekly change windows to ensure no negative impact to applications. Setting updates are verified the following day by the monitoring script to ensure updates are in place. Script variables associated with duration and cycle settings will be adjusted per the security plan annual review to ensure compliance with published policy.

Corrective Action 5: OMS will configure password settings to comply with Agency access control requirements for the password expiration, password reuse maximum, and inactive account time password settings.

Planned Completion Date: Completed. See attached for documentation.

Recommendation 6: Document the Integrated Risk Information System database's security controls, including password configuration settings, in a system security plan and work with the Office of Information Technology Operations to confirm those settings are reviewed as part of its annual security plan review process.

OMS Response: OMS agrees with this recommendation and will work with the ORD application owners to ensure documentation is updated in compliance with the Authorization to Use (ATU) process supporting the GSS. OITO reviews compliance with current published policy by validating settings against the policy during the annual review of security plans. Updates and changes resulting from this review are disseminated to the technical teams. OITO will review and improve communications between the security plan review teams and the technical teams following those reviews to ensure updates and changes are communicated properly and implemented in compliance with published policy.

Corrective Action 6: OMS will document the Integrated Risk Information System database's internal security controls, including password configuration settings, in a system security plan and work with the Office of Information Technology Operations to confirm those settings are reviewed as part of its annual security plan review process.

Planned Completion Date: December 30, 2024

Recommendation 7: Work with the Office of Mission Support to incorporate the Integrated Risk Information System database into the National Computer Center's Hosting System's security plan.

ORD Response: ORD concurs with this recommendation and proposes the following corrective action and completion date.

Corrective Action 7: ORD will work with OMS to obtain an Authorization to Use (ATU) approval via the Application Characterization Document (ACD) review process that is managed by OMS. This will incorporate the IRIS database into the National Computer Center's Hosting System's security plan.

Planned Completion Date: December 30, 2025

Attached please find specific comments on the Draft Report. If you have any questions regarding this response, please contact Caitlin Schneider, Office of Research and Development, Office of Resource Management, at ORD_AuditTeam@epa.gov or Afreeka Wilson, Office of Mission Support, at OMS_Audit_Coordination@epa.gov.

Attachment

cc: Wayne Cascio, ORD/CPHEA
Kay Holt, ORD/CPHEA
Kris Thayer, ORD/CPHEA
Samantha Jones, ORD/CPHEA
Vique Caro, ORD/OSIM
John Sykes, ORD/OSIM
John Steenbock, ORD/ORM
Heather Cursio, ORD/ORM
Caitlin Schneider, ORD/ORM
Afreeka Wilson, OMS
Darryl Perez, OMS
Marilyn Armstrong, OMS
OMS_Audit_Coordination
Sue Perkins, OCFO
Lasharn Barnes, OIG
Jeremy Sigel, OIG
Tertia Allen, OIG
Eric Lewis, OIG

Distribution

The Administrator
Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff for Management, Office of the Administrator
Agency Follow-Up Official (the CFO)
Assistant Administrator for Mission Support
Assistant Administrator and EPA Science Advisor for Research and Development
Principal Deputy Assistant Administrator for Mission Support
Principal Deputy Assistant Administrator and EPA's Chief Scientist for Research and Development
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Deputy Assistant Administrator for Mission Support
Deputy Assistant Administrator for Research and Development
Chief Information Officer and Deputy Assistant Administrator for Environmental Information, Office of Mission Support
Deputy Assistant Administrator for Administration and Resources Management, Office of Mission Support
Director, Office of Continuous Improvement, Office of the Chief Financial Officer
Director, Office of Resources and Business Operations, Office of Mission Support
Office of Policy OIG Liaison
Office of Policy GAO Liaison
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Mission Support
Audit Follow-Up Coordinator, Office of Research and Development

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit the OIG's whistleblower protection webpage.

Contact us:

Congressional Inquiries: OIG.CongressionalAffairs@epa.gov

Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epaoig.gov

Follow us:

X (formerly Twitter): @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epaoig.gov