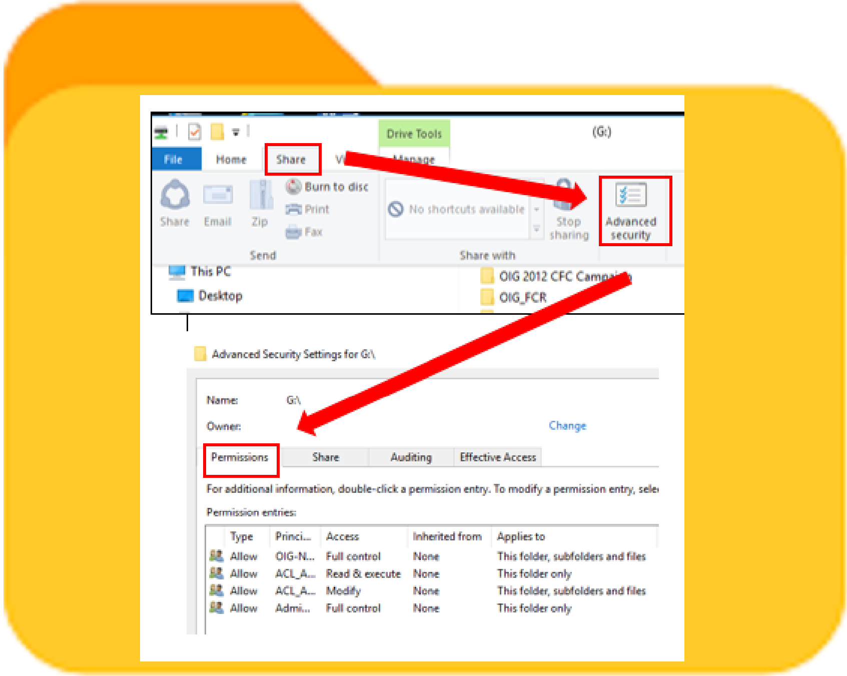
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Compliance with the law
Operating efficiently and effectively

Without a Process for Monitoring Sensitive Data, EPA Region 4 Risks Unauthorized Access to File Servers and Share Folders

Report No. 18-P-0234 **August 28, 2018**



Advanced Security Settings for G:\

Name: G:\

Owner:

For additional information, double-click a permission entry. To modify a permission entry, sele

Permission entries:

Type	Princi...	Access	Inherited from	Applies to
Allow	OIG-N...	Full control	None	This folder, subfolders and files
Allow	ACL_A...	Read & execute	None	This folder only
Allow	ACL_A...	Modify	None	This folder, subfolders and files
Allow	Admi...	Full control	None	This folder only

Report Contributors:

Rudolph M. Brevard
Iantha Maness
Christina Nelson
Jeremy Sigel
Sabrena Stewart

Abbreviations

AC	Access Control
AU	Audit and Accountability
DSS	Directory Service System
EPA	U.S. Environmental Protection Agency
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SEMS	Superfund Enterprise Management System
SP	Special Publication

Cover Image: Share folder permission example. (EPA OIG image)

Are you aware of fraud, waste or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, DC 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, DC 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

18-P-0234
August 28, 2018

At a Glance

Why We Did This Project

The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), conducted this audit to assess the EPA's implementation of security controls for agency file servers.

A file server provides file sharing services so that only authorized users can access, modify, store and delete files. File servers are considered components of an information system and therefore should meet the security guidance of National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

This report addresses the following:

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

Send all inquiries to our public affairs office at (202) 566-2391 or visit www.epa.gov/oig.

Listing of OIG reports.

Without a Process for Monitoring Sensitive Data, EPA Region 4 Risks Unauthorized Access to File Servers and Share Folders

What We Found

We determined that a share folder found on EPA Region 4 file servers did not comply with federal and agency guidance for access administration. The Region 4 share folder contained sensitive data, and the region did not have a process to monitor user activity or content in file servers' share folders.

Sensitive data are vulnerable to unauthorized disclosure without a tool or process in place to monitor user activity and access to share folders found on EPA Region 4 file servers.

Federal and agency guidance requires agencies to implement security controls for their information systems and related components. Information system components include file servers and the share folders they host.

Region 4 lacked documented procedures for EPA information technology security control requirements applicable to file servers and share folders. In addition, Region 4 lacked documented procedures for monitoring share folder access or content.

EPA data were vulnerable to unauthorized access because Region 4 did not create procedures to ensure that EPA security control requirements were implemented for file servers and share folders. The lack of procedures, combined with the lack of audit logging or an audit log review process, put the EPA at risk for unauthorized activity being undetected and uninvestigated.

Recommendation and Agency Corrective Actions Taken

We recommend that the Regional Administrator for Region 4 develop a process to approve and monitor access to share folder content that is consistent with requirements contained in National Institute of Standards and Technology Special Publication 800-53 and EPA information security procedures.

Region 4 agreed with our report and recommendation. The region completed all proposed corrective actions by August 14, 2018, and those actions satisfy the intent of the recommendation.

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

THE INSPECTOR GENERAL

August 28, 2018

MEMORANDUM

SUBJECT: Without a Process for Monitoring Sensitive Data, EPA Region 4 Risks Unauthorized Access to File Servers and Share Folders
Report No. 18-P-0234

FROM: Arthur A. Elkins Jr. Arthur A. Elkins

TO: Trey Glenn, Regional Administrator
Region 4

This is our report on the subject audit conducted by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). The project number for this audit was OA-FY17-0138. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position.

The Information Systems Management Branch within EPA Region 4 is responsible for implementing the recommendation in this report.

In accordance with EPA Manual 2750, your office completed acceptable corrective actions in response to the OIG recommendation. The recommendation is resolved, and no final response to this report is required. However, if you submit a response, 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.epa.gov/oig.

Table of Contents

Purpose 1

Background 1

Responsible Offices 2

Scope and Methodology 2

Results 3

EPA Region 4 Needs to Improve the Process for Verifying Access to SEMS Share Folder 4

No Process Is in Place to Review and Analyze Share Folders for Unauthorized Access 5

Conclusion 5

Recommendation 6

Agency Response and OIG Evaluation 6

Status of Recommendations and Potential Monetary Benefits 7

Appendices

A **Agency Response to Draft Report** 8

B **Distribution** 10

Purpose

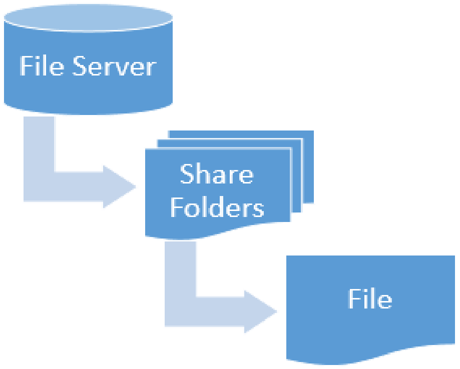
The U.S. Environmental Protection Agency (EPA), Office of Inspector General (OIG), sought to determine whether the EPA is implementing security controls for agency file servers.

Background

According to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-123, *Guide to General Server Security*, dated July 2008, a file server provides one or more services over a network as its primary function. A file server provides services where authorized users can access, modify, store and delete files.

As illustrated in Figure 1, file servers contain share folders. These share folders contain files that multiple users or groups can access based on their authorization. File servers are considered a component of an information system and therefore should meet security guidance of NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization*.

Figure 1: Interrelationship of a file, share folder and file server



Source: OIG image.

File servers can exist within the EPA's directory service system (DSS) or outside of the DSS. The EPA uses a commercial off-the-shelf product for its DSS. The EPA uses the DSS to centralize which type of servers can be accessed and which users are allowed access to the agency's network. The EPA also has stand-alone file servers outside of the DSS, which can be set up for a particular purpose or as part of an EPA application.

A *directory service system* provides a centralized location to store information about users, computers and other equipment on a network, as well as integrated services that are used to manage network users, services and devices.

The EPA's Superfund Enterprise Management System (SEMS) is the agency's system of record for the Superfund program. The SEMS contains the official inventory of Superfund sites, as well as documentation encompassing site cleanup activities at regional Superfund sites, contract documentation, enforcement records, and emergency response and contaminant information, among other items. The SEMS is key to the EPA meeting its responsibilities to federal agencies, Congress and the public regarding Superfund site remediation. The SEMS is also used for Freedom of Information Act requests, administrative records and litigation support.

Responsible Offices

The Office of Information Technology Operations, within the Office of Environmental Information, is responsible for implementing and managing the EPA's information technology (IT) infrastructure, which includes the agency's DSS and IT solutions. EPA program and regional offices are responsible for the administration of their own file servers and associated share folders. This responsibility includes controlling who can access the file servers and share folders. In EPA Region 4, personnel in the Information Systems Management Branch are responsible for managing these activities.

Scope and Methodology

We conducted this audit from February 2017 to June 2018 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We also obtained a population of file servers outside of the EPA's DSS, using survey responses from EPA program and regional offices' IT personnel responsible for administering file servers. During our audit fieldwork, we learned that users had migrated data on these servers to another technology. We followed up with system owners to gather an understanding of how they migrated the data.

We identified the population of EPA file servers, as of March 2017, from an Office of Environmental Information report on file servers within the EPA's DSS network, and we judgmentally selected 10 file servers from the EPA offices listed in Table 1. File servers were sampled based on the portion of the EPA file server population owned by the EPA program office/region and on their proximity to EPA headquarters, where our audit work was performed. We interviewed office personnel about file server access administration and the existence of share folders with sensitive information on their file servers.

Table 1: Sampled EPA program/regional office file servers on the DSS

Program/regional office	No. of file servers on the EPA's DSS network	No. of file servers sampled	No. of share folders with sensitive information hosted on sampled file servers
Office of Enforcement and Compliance Assurance	17	2	0
Office of Environmental Information	16	2	0
Office of Research and Development	37	4	0
Region 4	22	2	1

Source: OIG-created table.

Based on our initial interviews with EPA offices, we narrowed our scope to the Region 4 sampled share folder that stores scanned SEMS documents with sensitive data. We tested whether the share folder was in compliance with the following NIST SP 800-53 security controls:

- Access Control (AC)—Account Management.
    - AC-2b: Account manager assigned.
    - AC-2d: Specified authorized users of the system.
    - AC-2e: Authorized official approves accounts.
    - AC-2h: Notified managers of changes in user access.
    - AC-2i: Authorized information system access based on criteria.
    - AC-2j: Accounts reviewed for compliance with account management requirements.
- Audit and Accountability (AU)—Audit Events.
    - AU-2: Audit organization-defined events within the information system.
- AU—Audit Review, Analysis and Reporting.
    - AU-6: Audit records reviewed and analyzed for unusual activity.

Results

EPA Region 4 lacked implemented security controls for the sampled SEMS share folder. We found the conditions existed because Region 4 IT personnel lacked documented procedures for federal and agency IT guidance applicable to file servers and share folders. This lack of documentation included procedures for file servers and share folders that did or did not contain sensitive information.

The EPA's IT security procedures require system owners to comply with NIST controls for all EPA information and information systems. There were no procedures implemented to track share folder content due to Region 4's reliance on user discretion and the access certification process.

The file server with sensitive data was susceptible to compromise because of the lack of implemented security controls. Table 2 outlines NIST information system security controls reviewed and the compliance rate.

Table 2: Region 4 compliance with required NIST SP 800-53 access and audit and accountability controls

NIST 800-53 controls tested	Region 4 compliance
AC-2b: Account manager assigned.	Noncompliant
AC-2d: Specified authorized users of the system.	Noncompliant
AC-2e: Authorized official approves accounts.	Noncompliant
AC-2h: Notified managers of changes in user access.	Noncompliant
AC-2i: Authorized information system access based on criteria.	Noncompliant
AC-2j: Accounts reviewed for compliance with account management requirements.	Noncompliant
AU-2: Audit organization-defined events within the information system.	Noncompliant
AU-6: Audit records reviewed and analyzed for unusual activity.	Noncompliant

Source: OIG-created table.

EPA Region 4 Needs to Improve the Process for Verifying Access to SEMS Share Folder

EPA Region 4 personnel were not verifying that access to the SEMS share folder is granted to only authorized users based on a valid access authorization. Region 4 personnel assigned share folder access roles to employees through the SEMS User Request System. Region 4 personnel stated that there is no documented list of authorized approvers or account managers for share folder users. There also was no regular review of share folder access for compliance with account management requirements.

We found that share folder users were granted access without documented approval. In addition, share folders were not monitored for unusual activity or access to sensitive information.

NIST SP 800-53, security control AC-2, Account Management, requires valid access authorization, an assigned account manager, regular compliance review, and authorized approval for agency information system accounts. NIST SP 800-53, security control AU-2, Audit Events, requires certain organization-defined events to be audited. Security control AU-6, Audit Review, Analysis and Reporting, requires an organization to review and analyze information audit system records for indications of inappropriate or unusual activity.

The EPA Chief Information Officer Transmittal 2150-P-01.2, *Information Security—Access Control Procedures*, specifies that system owners shall review users' activities to enforce access controls. The Chief Information Officer Information Transmittal 2150-P-03.2, *Information Security—Audit and Accountability Procedures*, further requires an organization to review and analyze audit logs and records weekly for organization-defined events, such as indications of inappropriate or unusual activity and access to sensitive information.

The conditions existed because Region 4 personnel lacked documented procedures for EPA access administration or audit log requirements applicable to agency file servers and share folders. The EPA's IT security procedures state that system owners must comply with NIST requirements for all EPA information and information systems. However, those directives do not tell EPA offices how to specifically implement the procedures.

No Process Is in Place to Review and Analyze Share Folders for Unauthorized Access

There was no process in place to review and analyze share folder activity for unauthorized access or transactions. Region 4 personnel stated that adding or removing sensitive data in the share folder is entrusted to end users, whose compliance with agency information system access requirements is controlled by the SEMS User Request System certification process.

Region 4 personnel stated that it is the end users' responsibility to make only authorized transactions when storing data on the share folder. Region 4 personnel also stated that they only review the number and permissions of their share folders from a Microsoft Excel spreadsheet. However, the spreadsheet that Region 4 personnel created was only spot-checked on an ad hoc basis, and personnel did not document their review.

The agency's data were vulnerable to unauthorized access because Region 4 personnel did not create procedures for EPA security control requirements for file servers and share folders. The lack of documented procedures for EPA security controls also compromised the confidentiality and integrity of sensitive agency data stored on Region 4 share folders. Combined with the lack of audit logging or an audit log review process, the EPA risked unauthorized activity going undetected and uninvestigated.

Region 4 had not implemented any of the mandated NIST information system security controls we reviewed.

Conclusion

By not implementing mandatory NIST information security controls, EPA Region 4 risked the unauthorized disclosure of sensitive agency data.

Recommendation

We recommend that the Regional Administrator, Region 4:

1. Develop a process for approving and monitoring access to share folder content. The procedures should include a process to verify that personnel responsible for controlling access to file servers and share folders containing sensitive information implement access and audit log control procedures as required by National Institute of Standards and Technology Special Publication 800-53 and agency information security procedures.

Agency Response and OIG Evaluation

Region 4 agreed with the report's findings and recommendation. Region 4 indicated that it conducted an internal meeting to discuss the region's current procedures for managing access to share folders. Region 4 also documented standard operating procedures for approving and monitoring share folder content, which are consistent with NIST SP 800-53 requirements and approved by the acting Chief of the Information Systems Management Branch.

We believe that the actions taken satisfy the intent of the recommendation, and all corrective actions were completed by August 14, 2108. Appendix A contains the full written response from Region 4.

Status of Recommendations and Potential Monetary Benefits

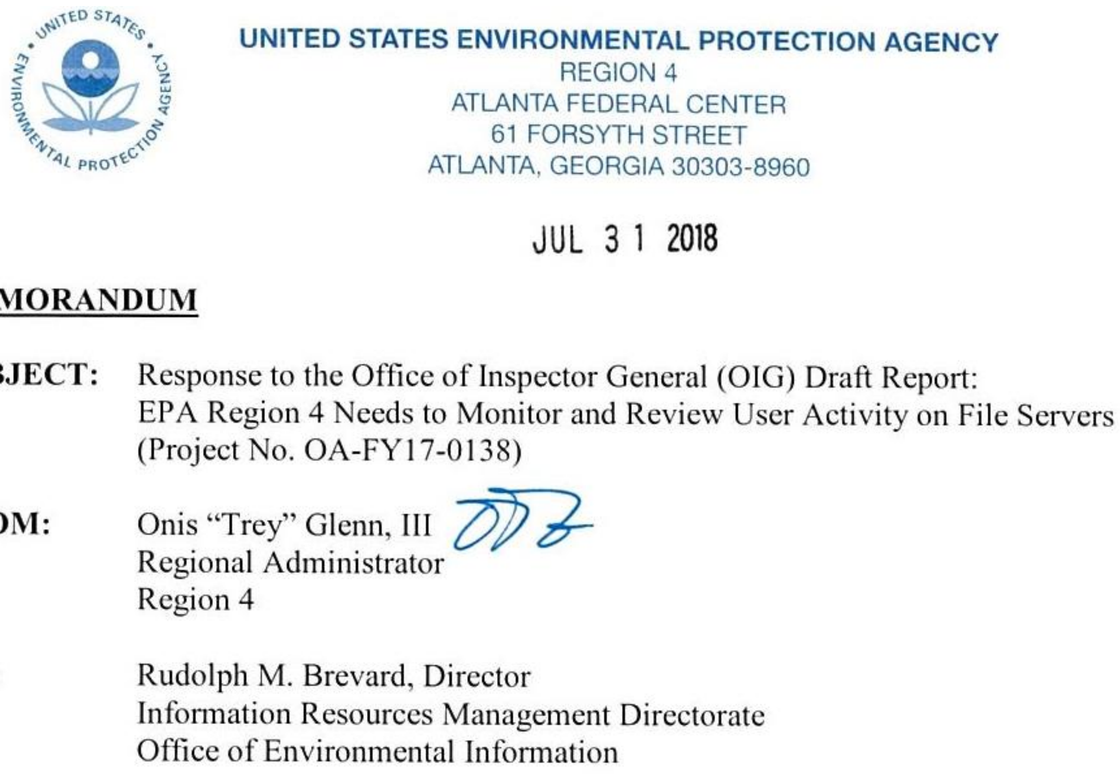
RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	6	Develop a process for approving and monitoring access to share folder content. The procedures should include a process to verify that personnel responsible for controlling access to file servers and share folders containing sensitive information implement access and audit log control procedures as required by National Institute of Standards and Technology Special Publication 800-53 and agency information security procedures.	C	Regional Administrator, Region 4	8/14/18	

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

Appendix A

Agency Response to Draft Report



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
REGION 4
ATLANTA FEDERAL CENTER
61 FORSYTH STREET
ATLANTA, GEORGIA 30303-8960

JUL 3 1 2018

MEMORANDUM

SUBJECT: Response to the Office of Inspector General (OIG) Draft Report:
EPA Region 4 Needs to Monitor and Review User Activity on File Servers
(Project No. OA-FY17-0138)

FROM: Onis "Trey" Glenn, III
Regional Administrator
Region 4

TO: Rudolph M. Brevard, Director
Information Resources Management Directorate
Office of Environmental Information

This memorandum is to acknowledge receipt of the subject draft report, dated July 5, 2018, written by the Office of Inspector General (OIG) of the U.S. Environmental Protection Agency (EPA). EPA Region 4 has reviewed the report in its entirety and concurs with the factual accuracy of each finding, as well as the recommendation provided by the OIG. In response to the OIG's recommendation, Region 4 has taken preliminary steps to implement corrective actions consistent with requirements of the National Institute of Standards and Technology (NIST), Special Publication 800-53, and agency information security procedures. Accordingly, please note the following corrective actions:

CORRECTIVE ACTIONS:

1. The Information Systems Management Branch (ISMB) of the Office of Policy and Management (OPM) will meet with the Superfund Enterprise Management System (SEMS) Administrator to discuss the Superfund Division's current procedures for managing access to shared folders. **Planned Completion Date:** Friday, July 13, 2018.

2. ISMB will develop official Standard Operating Procedures (SOPs) for SEMS management of shared folders which will include audit criteria, specific measures for managing access to folders, a detailed list of roles and responsibilities, and a process to verify personnel responsible for controlling access to file servers and shared folders containing sensitive data. The SOPs will align with the requirements and guidelines set

by the agency’s information security procedures and the National Institute of Standards and Technology (NIST) controls.
Planned Completion Date: Friday, August 31, 2018

Should any questions or concerns arise regarding the above planned corrective actions, please contact Don Westra, Acting Chief, ISMB, at 404-562-8129 or Westra.Don@epa.gov.

cc: Kristy Eubanks
Rickey Felton
Kathie Johnson
Keith Mills
Jeremy Sigel
Pareasa Stevens
Don Westra

Distribution

The Administrator
Deputy Administrator
Special Advisor, Office of the Administrator
Chief of Staff
Regional Administrator, Region 4
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Deputy Regional Administrator, Region 4
Principal Deputy Assistant Administrator and Deputy Chief Information Officer, Office of Environmental Information
Chief Information Security Officer, Office of Information Security and Privacy, Office of Environmental Information
Director, Office of Continuous Improvement
Director, Information Systems Management Branch, Region 4
Director, Office of Information Technology Operations, Office of Environmental Information
Director, Office of Regional Operations
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Region 4
Audit Follow-Up Coordinator, Office of Environmental Information
Public Affairs Officer, Region 4