Office of Inspector General | United States Postal Service

Management Alert

Workplace Environment Tracking System (WETS) User Access

Report Number 22-099-R22 | May 10, 2022

Table of Contents

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

May 10, 2022

MEMORANDUM FOR: THOMAS J. BLUM
ACTING VICE PRESIDENT, LABOR RELATIONS

Margaret B. McDavid

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
Inspection Service & Cybersecurity and
Technology Directorate

SUBJECT: Management Alert – Workplace Environment Tracking System (WETS) User Access (Report Number 22-099-R22)

This management alert presents issues identified during our ongoing audit of the U.S. Postal Service's Response to Sexual Harassment complaints (Project Number 21-173). Our objective is to provide Postal Service officials immediate notification of risks associated with user access to the Workplace Environment Tracking System (WETS). These issues require immediate attention and remediation.

We appreciate the cooperation and courtesies provided by your staff. If you have questions or need additional information, please contact Elizabeth Kowalewski, Director, Inspection Service, or me at 703-248-2100.

Attachment

cc: Corporate Audit Response Management
Postmaster General

Results

Introduction

This management alert presents issues the U.S. Postal Service Office of Inspector General (OIG) identified during our ongoing audit of the *U.S. Postal Service's Response to Sexual Harassment Complaints* (Project Number 21-173). Our objective is to provide Postal Service officials immediate notification of these issues and make recommendations for corrective action.

We identified these issues while conducting a performance audit in accordance with generally accepted government auditing standards. Those standards require that we perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal agencies, including the Postal Service, are required to comply with Title VII of the Civil Rights Act of 1964, which makes it illegal for employers to allow anyone to be sexually harassed at work, regardless of sex, gender, or sexual orientation. The Postal Service launched the Workplace Environment Tracking System (WETS) on August 1, 2013, to provide a central nationwide repository for tracking harassment allegations and workplace environment issues. This system was designed to enable the Postal Service to identify trends and develop preventative measures against workplace harassment.

In accordance with Postal Service policy, area and district Human Resources managers (or their designees) use WETS to create and update Postal Service workplace harassment cases. To access WETS, users submit an access request through the eAccess system. The eAccess system communicates with WETS to confirm that requesters are approved to receive system access for the selected area(s) and district(s) associated with their user role.

Findings Summary

We determined that users could not obtain new access or change existing access to WETS for approximately eight months and found that management could not readily explain what caused the issue or its effect on the harassment data contained in WETS. Further, we determined the WETS Information Technology (IT) team did not comply with Postal Service password security requirements.

Finding #1: WETS User Access Discrepancies

During the course of our work in support of the OIG's *U.S. Postal Service's Response to Sexual Harassment Complaints* audit (Project 21-173), we determined that users were unable to obtain new access or change existing access to WETS for approximately eight months. While the Postal Service took corrective action in December 2021 and users can now obtain WETS access or change their user role, management could not readily explain what caused the access issue or what effect it may have had on the harassment data in WETS.

Specifically, in August 2020, the Postal Service began to realign its areas and districts, ultimately consolidating seven postal areas into four, and 67 districts into 50. However, after changes in eAccess went into effect in May 2021, user roles in eAccess and Postal Service locations in WETS did not match until December 2021. When users submitted their WETS access requests in eAccess during this period, the Postal Service denied the requests because the information in the two systems was not in sync and requests could not be processed.

During our work, we identified two problems that contributed to the WETS user access issue. First, as discussed in Finding 2, the WETS IT team had to contact a former employee to obtain the password required to make necessary changes to the WETS Oracle database. Second, we found that the Postal Service installed a new WETS production server without submitting a Network Connectivity Review Board (NCRB) ticket for eAccess connectivity. This caused an existing Postal Service firewall to block communication between WETS and eAccess and contributed to further delays in resolving the user access issue. Upon introduction of a new server, the Postal Service must submit a NCRB ticket to identify the requirements for connectivity. In December 2021, the WETS IT team submitted the required NCRB ticket, thereby resolving the WETS user access issue. Therefore, we are not making a recommendation on this issue.

We also determined that during the eight months when users could not request access or change their user role, the Postal Service accumulated a backlog of 65 pending user access requests. Further, in fiscal year (FY) 2021, the total number of WETS cases decreased by 28 percent compared to FY 2020. In contrast, another postal system database containing data on similar types of cases saw significant increases during the same time period.

According to the *Standards for Internal Control*, management should evaluate and document deficiencies and their corrective actions on a timely basis.[1] The *Standards for Internal Control* also state that management should use quality information to make informed decisions and achieve the entity's objectives. Among other things, quality information is complete, accurate, and provided on a timely basis.[2]

However, management did not conduct an after-action report to thoroughly document the causes of or solutions to the user access issue or its effect on the harassment data in WETS. While we were able to identify two factors that contributed to the WETS user access issue, without a documented after-action report, management lacks assurance that appropriate steps have been taken to prevent this issue from occurring again. Additionally, without fully evaluating the impact of the access issue on users and WETS data, management cannot rely on WETS to meet their tracking and reporting requirements for workplace harassment in FY 2021.

Recommendation #1

We recommend the **Vice President, Labor Relations**, create an after-action report of the Workplace Environment Tracking System access issue documenting how the access issue occurred, corrective actions taken to resolve the problem, impact of the issue on user access and data quality, and any controls and policies implemented to prevent the issue in future.

Recommendation #2

We recommend the **Vice President, Labor Relations**, ensure all cases of workplace harassment that occurred during the system failure are recorded in the Workplace Environment Tracking System.

Finding #2: Oracle Password

We found that the WETS IT team did not comply with Postal Service password security requirements. Specifically, despite using a username and password that is not assigned to a specific user for the WETS Oracle administrator account, the team did not have the password to log into the WETS Oracle database in the development environment. The team had to contact a retired Postal Service employee to obtain the password before they could update area and district names and user roles in WETS to resolve the system's access issue.

Per Postal Service policy, Oracle database account passwords are non-expiring and are controlled by the Postal Service's Database Systems and Services (DBSS) group. Policy requires the DBSS group to change the database password when personnel with access to the account leaves or transfers as a compensating control for non-expiring passwords.[3] However, in attempting to resolve the user access issue, the WETS IT team discovered that the only person with knowledge of the administrator account password for the WETS Oracle database's development environment had retired from the Postal Service in November 2021 without transferring the login credentials to another employee.

After we brought this issue to management's attention, the WETS IT team submitted a ticket to change the WETS Oracle password in the development environment, which was successfully completed in April 2022. Therefore, we are not making a recommendation on this matter. However, we plan to conduct future work to further assess the Postal Service's practice of using database administrator accounts that are not assigned to specific users.

1 GAO, *Standards for Internal Control*, Sections 17.05 and 17.06.
2 GAO, *Standards for Internal Control*, Sections 13.01 and 13.05.
3 Handbook AS-805, *Information Security*, Section 9-6.1.7.

Although the password for the WETS Oracle administrator account has been changed, without the required controls in place to ensure that only authorized personnel have access to key data systems, the Postal Service is at an increased risk of security violations which could result in the loss or misuse of data.

> **Recommendation #3**
> We recommend the **Vice President, Labor Relations**, implement monitoring controls to ensure the password for the Workplace Environment Tracking System Oracle database account is changed when personnel with access leave or transfer.

Additional information or recommendations regarding the issues addressed in this management alert may also be included in the final report resulting from our related ongoing audit.

Management's Comments

Management agreed with recommendation 1, partially agreed with recommendation 2, and disagreed with recommendation 3. In subsequent correspondence, management agreed with findings 1 and 2.

Regarding finding 1, in their formal comments, management stated that the user access issue did not affect the data integrity in WETS. However, in a subsequent response, management agreed with our finding that new users could not obtain access to WETS and existing users could not modify their user access for approximately eight months.

Regarding recommendation 1, management agreed to complete an after-action report to document how the access issue occurred, corrective actions taken to resolve the problem, impact of the issue on user access and data quality, and any controls and policies implemented to prevent the issue in the future. The target implementation date is September 30, 2022.

Regarding recommendation 2, management disagreed that WETS data was affected by the user access issue but agreed to issue a memorandum to the field recommending that field employees perform follow-up activities to ensure all cases are recorded in WETS consistent with Postal Service policy. The target implementation date is July 31, 2022.

Regarding finding 2, in their formal comments, management stated that existing controls are sufficient to ensure secured access to WETS. Further, management stated that the WETS database is not an Oracle database but a Structured Query Language (SQL) database. However, in a subsequent response, management agreed with our finding that they did not immediately change a WETS Oracle database password when an employee retired.

Regarding recommendation 3, management disagreed that additional monitoring controls were required to ensure that the WETS database password is changed when employees transfer or depart the agency. Management stated that current Postal Service policy controls are sufficient.

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments generally responsive to recommendations 1 and 2, and corrective actions should resolve the issues identified in the alert. We view the disagreement on recommendation 3 as unresolved and plan to pursue it through the audit resolution process.

Regarding recommendation 2, management did not provide documentation to support their assertion that the user access issue we identified did not impact the data integrity of the WETS system. In management's response to recommendation 1, they agreed to evaluate the impact of the access issue on WETS data. Until they complete this assessment, management lacks assurance that WETS contained all harassment data during the time of the WETS access issue.

Regarding finding 2, SQL is the programming language the WETS Oracle database uses to manage and organize data. Documentation the WETS IT team provided us related to steps taken to resolve the user access issue clearly identifies WETS as an Oracle database. Specifically, WETS IT team members were required to update the SQL code by logging into the WETS Oracle database using the administrator account.

Regarding recommendation 3, although management stated that existing controls in Handbook AS-805, Section 9-6.1.7 are sufficient to ensure the security of the WETS Oracle database, as stated in our report these controls were not followed. Without additional monitoring controls, the Postal Service is at an increased risk of security violations, which could result in the loss or misuse of data.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendix A: Additional Information

Scope and Methodology

Our scope included data integrity and IT security controls in place for the WETS system.

To accomplish our objective, we:

- Obtained Postal Service criteria related to servers, network changes, and Oracle administrator accounts and reviewed it to identify internal controls.
- Interviewed the acting data analytics specialist to understand the issues in obtaining access to the WETS database.
- Reviewed the acting data analytics specialist's notes from meetings with the Postal Service to obtain a greater understanding of the user access issue.
- Interviewed the WETS IT team to obtain an understanding of the user access issue and the steps they took to mitigate the issue. We also reviewed supporting evidence, such as email correspondence and IT tickets, to verify the accuracy of the WETS technical team's description of the issue.
- Interviewed eAccess IT team members to obtain an understanding of the user access issue and the steps they took to mitigate the issue. We also reviewed supporting evidence, such as email correspondence and IT tickets, to verify the accuracy of the eAccess technical team's description of the issue.

We conducted the work for this alert from March through May 2022 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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.

On March 9, 2022 we notified management that we would be issuing a draft of this management alert. We discussed our observations and conclusions with management on March 30, 2022, and included their comments where appropriate.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews related to the objective of this audit conducted within the last five years.

Appendix B: Management's Comments

THOMAS J. BLUM
VICE PRESIDENT, LABOR RELATIONS (A)

UNITED STATES POSTAL SERVICE

April 29, 2022

JOHN CIHOTA
DIRECTOR, AUDIT SERVICES

SUBJECT: Workplace Environment Tracking System (WETS) User Access
(Project Number 22-099-DRAFT)

Thank you for the opportunity to review and respond to the subject Office of Inspector General (OIG) management alert. As more thoroughly discussed below, the Postal Service agrees in part and disagrees in part with the OIG's recommendations in the draft management alert.

The Postal Service agrees that an after-action report on the Workplace Environment Tracking System (WETS) access issue will be helpful in documenting lessons learned and potentially identifying additional controls that could reduce future compliance issues. However, the Postal Service disagrees that any further action is required to confirm the data integrity in WETS. The access issue following the national Postal Service restructuring did not impact case entry into WETS due to the Postal Service's existing procedures and continued system access was available within the districts. Additionally, the OIG recommended that the Postal Service implement monitoring controls to ensure the password for the WETS Oracle database account is changed when personnel with access leave or transfer. Please note, management disagrees with OIG's recommendation. The existing controls found in AS805 9-6.1.7 and 9-6.1.8 are sufficient to ensure secured access to WETS. The business need does not exist to justify the additional new controls to prevent secured access issues in the future.

In addition to the responses to the OIG's specific recommendations, the Postal Service also notes significant concern with a statement in the draft report that indicates, "In contrast, another postal system database contained similar types of cases saw significant increases during the same time period." The OIG has not identified or provided the name of the other database or additional specific information to enable a specific response to this assertion. The Postal Service has no data raising doubt that WETS maintains the most-accurate data for the four workplace environment processes. WETS is the centralized repository for this information and no other postal system is intended to be used to track the same information in the same manner. Therefore, the Postal Service has no basis to conclude the agency controls another system storing the identical data.

Following please find the Postal Service's response in reference to the OIG's specific recommendations:

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4100

Recommendation #1:

"We recommend the VP, Labor Relations, create an after-action report of the Workplace Environment Tracking System access issue documenting how the access issue occurred, corrective actions taken to resolve the problem, impact of the issue on user access and data quality, and any controls and policies implemented to prevent the issue in the future."

Management Response/Action Plan:

Management agrees with this recommendation.

Labor Relations has already coordinated with Technology Applications and resolved the access issue. An after-action report will be completed to document how the access issue occurred, corrective actions taken to resolve the problem, impact of the issue on user access and data quality, and any controls and policies implemented to prevent the issue in the future.

Target Date: September 30, 2022

Recommendation #2:

"We recommend the VP, Labor Relations, ensure all cases of workplace harassment that occurred during the system failure are recorded in the Workplace Environment Tracking System."

Management Response/Action Plan:

Management disagrees with this recommendation because workplace harassment cases continued to be recorded in WETS despite the access issue, so no further action is warranted.

As noted above, no system failure occurred that precipitated the issues identified in the subject management alert. Rather, during the national restructuring, some users could not obtain new access or modify existing access for WETS. However, this did not have an impact on existing users, who continued to enter cases into WETS under the Postal Service's existing protocols.

While many Postal Service's districts were consolidated, there were no previously unaccounted for geographic locations. To account for transitions of responsibility associated with the reduction in districts, the Postal Service issued a memorandum to the Directors, Field Human Resources (Region), Managers, Human Resources (Districts), and Directors, Field Labor Relations, advising the consolidated districts to close IMI, WHFF, TACT, and WEI cases and send hardcopy files to the appropriate district personnel for continued tracking. Under this approach, the newly determined 50 districts maintained access to WETS to create entries, and follow-up entries for IMI, WHFF, TACT, and WEI cases in the system also continued.

Nevertheless, the Vice President, Labor Relations, will issue a memorandum reiterating the importance of entering all IMIs into the WETS system and performing follow-up activities as applicable to ensure all cases have been timely entered and updated in accordance with postal policy.

Target Date: July 31, 2022.

Recommendation #3:

"We recommend the VP, Labor Relations, implement monitoring controls to ensure the password for the Workplace Environment Tracking System Oracle database account is changed when personnel with access leave or transfer."

Management Response/Action Plan:

Management disagrees with this recommendation. The Microsoft SQL Database is under the operational control of the Vice President, Technology Applications.

The WETS application utilizes Microsoft SQL Database rather than Oracle. The password for "the Workplace Environment Tracking system Oracle database account" was not part of the access issue or the resolution. The Chief Information Officer addressed the immediate issue by changing the password used by the WETS application backend process to read data from the eAccess development database according to existing controls. The existing controls required in AS805 9-6.1.7 and 9-6.1.8 are sufficient. There is no need for additional controls to be added to prevent a reoccurrence of this issue in the future.

Thank you for the opportunity to review and respond to your concerns and recommendations.

Thomas J. Blum

cc: CARM
Ms. Wattree-Bond
Ms. Chounet
Mr. Ellis

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100