



Memorandum from the Office of the Inspector General

January 29, 2019

Andrea S. Brackett, WT 5D-K
Wilson Taylor III, WT 7D-K

REQUEST FOR MANAGEMENT DECISION – AUDIT 2018-15531 – HUMAN RESOURCE SYSTEM PERSONALLY IDENTIFIABLE INFORMATION ACCESS CONTROL

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions or wish to discuss our findings, please contact Melissa L. Conforti, Senior Auditor, at (865) 633 7383 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633 7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)
WT 2C-K

MLC:KDS
Attachment

cc (Attachment):

TVA Board of Directors
Clifford L. Beach Jr, WT 6A-K
Janet J. Brewer, WT 7C-K
Susan E. Collins, LP 6A-C
Trevor L. Cothron, SP 2A-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MP 3B-C
Megan T. Flynn, LP 3A-C
William D. Johnson, WT 7B-K
J. Denise Jones, WT 4A-K
Dwain K. Lanier, MR 6D-C

Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Todd E. McCarter, MP 2C-C
Philip D. Propes, SP 2N-C
Sherry A. Quirk, WT 7C-K
John M. Thomas III, MR 6D-C
Scott W. Tiemeyer, LP 3A-C
Rebecca C. Tolene, WT 7B-K
Diane T. Wear, WT 4B-K
OIG File No. 2018-15531



Office of the Inspector General

Audit Report

To the Director, TVA Cybersecurity,
and to the Vice President, Human
Resources Operations Services and
Ombudsman

HUMAN RESOURCE SYSTEM PERSONALLY IDENTIFIABLE INFORMATION ACCESS CONTROL

Audit Team
Melissa L. Conforti
Michael P. Anderson
Weston J. Shepherd

Audit 2018-15531
January 29, 2019

ABBREVIATIONS

HR	Human Resource
IT	Information Technology
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
RPII	Restricted Personally Identifiable Information
SOX	Sarbanes-Oxley
SPP	Standard Programs and Processes
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
BACKGROUND.....	1
OBJECTIVE, SCOPE, AND METHODOLOGY	1
FINDINGS	1
PREVENTATIVE ACCESS CONTROLS NEED IMPROVEMENT.....	2
No Active Monitoring of Privileged User Accounts.....	2
Noncompliant Access Reviews.....	2
Outdated System Authorization	3
DETECTIVE AUDIT AND ACCOUNTABILITY CONTROLS NEED IMPROVEMENT	3
Lack of Internal Monitoring of Exported HR System RPII Within the Agency.....	3
Gaps between TVA’s Policies and NIST PII Best Practices.....	3
RECOMMENDATIONS	4

APPENDICES

- A. OBJECTIVE, SCOPE, AND METHODOLOGY
- B. MEMORANDUM DATED JANUARY 18, 2019, FROM WILSON TAYLOR III AND ANDREA S. BRACKETT TO DAVID P. WHEELER



Audit 2018-15531 – Human Resource System Personally Identifiable Information Access Control

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Tennessee Valley Authority (TVA) implemented a human capital management system that integrates people, payroll, and learning processes in 2013. This human resource (HR) system is the authoritative source of all people information for TVA. The HR system provides business functionality associated with the implementation of several modules, including HR, benefits administration, and payroll. Hence, personally identifiable information (PII) is contained in the HR system at TVA.

General information technology (IT) access controls, such as access management and the monitoring of access and exported data, are necessary to protect unauthorized access to PII and prevent disclosure of such information. TVA has Standard Programs and Processes (SPP) that define the process requiring IT access controls to protect TVA information. In addition, the National Institute of Standards and Technology (NIST)ⁱ has information security standards and guidelines of security and privacy controls for federal information systems and organizations.

We scheduled this audit as part of our annual audit plan due to the risk of protected information disclosure.ⁱⁱ Our objective was to determine if TVA has internal controls in place to prevent, detect, and report unauthorized access and disclosure of HR system PII. Our audit scope was PII within the HR system.

What the OIG Found

We found TVA has weaknesses in its internal controls to prevent and detect unauthorized access and disclosure of HR system PII. Specifically, we found (1) no active monitoring of privileged user accounts, (2) noncompliant access reviews, (3) an outdated system authorization, (4) a lack of monitoring when electronically sharing HR system restricted personally identifiable information (RPPII)ⁱⁱⁱ within the agency, and (5) gaps between TVA policies and NIST PII best practices.

ⁱ NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, January 22, 2015.

ⁱⁱ Protected information disclosure includes the willful and accidental disclosure of confidential or sensitive business information and assets and PII.

ⁱⁱⁱ RPPII is information the unauthorized disclosure of which could create a substantial risk of identity theft (e.g., social security number, bank account number, certain combinations of PII).



Audit 2018-15531 – Human Resource System Personally Identifiable Information Access Control

EXECUTIVE SUMMARY

What the OIG Recommends

We made five specific recommendations to management to improve internal controls to prevent and detect unauthorized access and disclosure of HR system RPII, including implementing monitoring of privileged user accounts and electronically shared RPII within the agency. Our specific recommendations are included within the report.

TVA Management's Comments

In response to our draft audit report, TVA management provided additional documentation that confirmed the (1) HR system was authorized in July 2018, (2) NIST best practice control gaps were documented in TVA's Consolidated Control Catalog and Enterprise Process Implementation documents, and (3) access issues had been remediated. TVA agreed with our remaining findings and recommendations and requested two of our recommendations be assigned to HR rather than IT. In addition, TVA management requested we add information to clarify three of the findings. See Appendix B for TVA management's complete response.

Auditor's Response

We reviewed additional documentation provided by TVA management and determined that prior to the date of our draft report the (1) HR system had been reauthorized, and (2) NIST control gaps were documented in TVA's Consolidated Control Catalog and Enterprise Process Implementation documents. Accordingly, no further action is required for these two findings, and we removed our recommendations. We also confirmed the access issues had been remediated and no further action is required by TVA. In addition, we addressed the two recommendations to HR and clarified the three findings as requested.

BACKGROUND

The Tennessee Valley Authority (TVA) implemented a human capital management system that integrates people, payroll, and learning processes from beginning to end in 2013. This human resource (HR) system is the authoritative source of all people information for TVA. The HR system provides business functionality associated with the implementation of several modules, including HR, benefits administration, and payroll. Hence, TVA employee personally identifiable information (PII) is contained in the HR system.

General information technology (IT) access controls, such as access management and the monitoring of access and exported data, are necessary to protect unauthorized access to PII and prevent disclosure of such information. TVA has Standard Programs and Processes (SPP) that define the required general IT access controls to protect TVA information. In addition, the National Institute of Standards and Technology (NIST)¹ has information security standards and guidelines of security and privacy controls for federal information systems and organizations.

We scheduled this audit as part of our annual audit plan due to the risk of protected information disclosure.²

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA has internal controls in place to prevent, detect, and report unauthorized access and disclosure of HR system PII. Our audit scope was PII within the HR system. A complete discussion of our audit objectives, scope, and methodology is included in the Appendix.

FINDINGS

In summary, we found TVA has weaknesses in its internal controls to prevent and detect unauthorized access and disclosure of HR system PII. Specifically, we found (1) no active monitoring of privileged user accounts, (2) noncompliant access reviews, (3) an outdated system authorization, (4) a lack of monitoring when electronically sharing HR system restricted personally identifiable information (RPII)³ within the agency, and (5) gaps between TVA policies and NIST PII best practices.

¹ NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, January 22, 2015.

² Protected information disclosure includes the willful and accidental disclosure of confidential or sensitive business information and assets and PII.

³ RPII is information the unauthorized disclosure of which could create a substantial risk of identity theft (e.g., social security number, bank account number, and certain combinations of PII).

PREVENTATIVE ACCESS CONTROLS NEED IMPROVEMENT

Preventative access controls for minimizing unauthorized access and disclosure of PII include current system authorizations; comprehensive policies; appropriate processes for granting, changing, and terminating user access; and periodic access reviews for reasonableness and segregation of duties. Although access was appropriately provisioned as designed by TVA-SPP-12.003, *IT Account Management*, with the security concepts of least privilege⁴ and need-to-know,⁵ we found weaknesses in monitoring of privileged user accounts and access review compliance as well as an outdated system authorization.

No Active Monitoring of Privileged User Accounts

General IT access controls defined by NIST include segregation of duties. These controls address the potential for abuse of authorized privileges and reduce the risk of malicious user activity without collusion. We reviewed a listing of all users with access to HR system data containing PII and determined access was generally segregated. Although access reviews were performed quarterly during our segregation of duties testing, we found inadequate monitoring of privileged accounts to prevent potential misuse of authorized access and detect unauthorized changes.

Specifically, we found five HR system administrators had privileged user accounts and could add, change, and delete HR-related information, which increases the risk for a potential of abuse of authorized privileges. According to TVA HR personnel, this level of access was appropriate for the job duties required of these five individuals. Although changes are captured in an audit table, the changes in the table are not actively monitored, which increases the risk of unauthorized changes not being detected.

Noncompliant Access Reviews

General IT access controls in NIST include access reviews that are also required by TVA-SPP-12.003 and TVA Sarbanes-Oxley (SOX) control documentation. Access reviews verify and validate that continued account user access to information systems is appropriate and help implement the principle of least privilege based on business need and segregation of incompatible roles and functions. We found quarterly HR system access reviews for HR users with elevated access beyond self-service were routinely occurring and requested access changes were processed. However, the reviews did not consistently involve the managers of those individuals who had access to the system as required by the SPP. In addition, the SOX control documentation did not define the managers required to review the access, so we could not determine if the reviews were being conducted by the appropriate TVA managers in accordance with the SOX control documentation.

⁴ Least privilege is the principle that a security architecture should be designed so each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

⁵ Need-to-know is a method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more.

General IT access controls in NIST include that managers should be notified when users are transferred, terminated, or their need-to-know changes to ensure timely termination of access to sensitive information. We reviewed the listing of all HR system users with access to data containing PII for reasonableness. While we determined the access was generally reasonable, we identified two employees who changed positions in 2017 and no longer needed assigned access. According to TVA IT personnel, when an employee is transferred or promoted within TVA, an e-mail notification should be sent to the user's former and current supervisor stating what access the employee was assigned so necessary changes can be identified. However, the two current supervisors stated they did not know the employees had this access and agreed it was no longer needed.

Outdated System Authorization

According to TVA-SPP-12.800, *Risk Management Framework*, TVA systems are authorized to operate for a specified period of time that should not exceed 3 years. The most recent system authorization issued for the HR system was completed on December 20, 2013, and was scheduled for reauthorization no later than December 20, 2016. The reauthorization has not yet occurred. According to TVA IT personnel, they are currently in the process of updating the system authorization.

DETECTIVE AUDIT AND ACCOUNTABILITY CONTROLS NEED IMPROVEMENT

Detective audit and accountability controls for minimizing unauthorized access and disclosure of PII include (1) comprehensive policies, (2) logging, and (3) monitoring and reporting suspicious activity. Although TVA has policies for these detective controls, we found (1) a lack of monitoring when electronically sharing HR system RPII within the agency and (2) gaps between TVA policies and NIST PII best practices.

Lack of Internal Monitoring of Exported HR System RPII Within the Agency

General IT audit and accountability controls in NIST include (1) logging access to PII and (2) monitoring and reporting suspicious activity when PII is shared electronically among internal and external users. We found TVA has processes to (1) log direct access to RPII in the HR system and (2) monitor, examine, and report for suspicious activity containing RPII when shared with external users. However, TVA does not have processes to monitor RPII electronically shared with internal users, which increases the risk of disclosing RPII to personnel who do not have a need-to-know. TVA is currently in the process of documenting processes and fully implementing a data loss prevention tool to monitor, examine, and report when RPII is shared electronically within the agency.

Gaps Between TVA's Policies and NIST PII Best Practices

General IT controls for minimizing unauthorized access and disclosure of PII are included in NIST best practices. We performed a gap analysis of TVA

documented policies against the NIST PII best practices. We found 4 of 55 identified best practices were not reflected by current TVA policy documentation. The specific controls not reflected by current TVA policy documentation have been shared with TVA management. Lack of documentation of controls could result in disclosure of protected information.

Subsequent to our draft audit report, TVA management provided additional documentation showing the best practice controls were documented. We reviewed the documentation and concur that 3 of the 4 best practice controls were reflected in TVA documentation. The remaining control was considered low risk and no additional action is required by TVA.

RECOMMENDATIONS

We recommend the Director, TVA Cybersecurity:

1. Complete planned actions to document and fully implement the data loss prevention tool to monitor, detect, report, and notify when RPII is shared electronically.

We recommend the Vice President, HR Operations Services and Ombudsman:

2. Implement a process to monitor the HR system for changes made by HR system administrators.
3. Ensure access reviews of users with elevated access beyond self-service are consistently performed by the appropriate TVA managers and coordinated to involve the managers of those individuals with access to the application, as required by TVA-SPP-12.003.
4. Update SOX documentation to include the access review process being performed, including a list to define appropriate managers to perform the access reviews.
5. Remove the access for the two individuals identified who transferred and no longer have a need-to-know.

TVA Management's Comments – In response to our draft audit report, TVA management provided additional documentation that confirmed the (1) HR system was authorized in July 2018, (2) NIST best practice controls were documented in TVA's Consolidated Control Catalog and Enterprise Process Implementation documents, and (3) access issues for the two identified individuals had been remediated. TVA agreed with our remaining findings and recommendations and requested two of the recommendations (recommendations 2 and 3 above) be assigned to HR rather than IT. In addition, TVA management requested we clarify three of the findings to state the (1) specific team whose user accounts were not being monitored (HR system

administrators), (2) specific access reviews not being consistently performed in accordance with TVA policy (administrator reviews of HR users with elevated access beyond self-service), and (3) type of PII is being referenced (RPII). See Appendix B for TVA management's complete response.

Auditor's Response – We reviewed additional documentation provided by TVA management and determined that prior to the date of our draft audit report, the (1) HR system had been reauthorized, and (2) NIST control gaps were documented in TVA's Consolidated Control Catalog and Enterprise Process Implementation documents. Accordingly, no further action is required for these two findings and we removed our recommendations. We also confirmed the access issues with the two individuals had been remediated and no further action is required by TVA. In addition, we addressed the two recommendations (recommendations 2 and 3) to HR and clarified the three findings as requested.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if the Tennessee Valley Authority (TVA) has internal controls in place to prevent, detect, and report unauthorized access and disclosure of human resource (HR) system personally identifiable information (PII). Our audit scope was PII within TVA's HR system. We did not evaluate the interfacing systems to the HR system. Fieldwork was performed from June 2018 through October 2018.

To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes (SPP) to obtain an understanding of the related information technology (IT) processes, including:
 - TVA-SPP-12.002, *TVA Information Management Policy*
 - TVA-SPP-12.003, *IT Account Management*
 - TVA-SPP-12.005, *Enterprise Cybersecurity Monitoring Program*
 - TVA-SPP-12.006, *Cyber Incident Response*
 - TVA-SPP-12.008, *Cybersecurity Policy*
 - TVA-SPP-12.501, *TVA Privacy Program*
 - TVA-SPP-12.800, *Risk Management Framework*
- Identified applicable PII best practices in the National Institute of Standards and Technology (NIST)¹ and performed a gap analysis of applicable TVA SPPs.
- Reviewed the listing of all three HR system users who had a change in access to PII to determine if proper approval was obtained prior to access being changed between January 1, 2018, and July 31, 2018.
- Compared the listing of all 420 HR system users who had access to PII as of June 15, 2018, to the listing of active personnel to determine if any users were not active.
- Reviewed the listing of all 420 HR system users who had access to PII as of June 15, 2018, to determine if (1) access was reasonable and segregated and (2) duplicate or shared accounts existed.
- Reviewed a systematic sample of ten HR system users who had access to PII to determine if proper approval was obtained prior to access being granted between January 1, 2018, and July 31, 2018. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Reviewed the fiscal year 2018 2nd and 3rd quarters' (as of March 29, 2018, and July 27, 2018, respectively) HR system access reviews to determine if access reviews were working as intended.

¹ NIST Special Publication 800-53 (Revision 4), *Security and Privacy Controls for Federal Information Systems and Organizations*, January 22, 2015.

- Interviewed TVA HR and IT personnel responsible for HR system access.
- Inquired with various TVA HR and IT personnel responsible for HR system user security.
- Performed a walkthrough of the HR system to observe the process for setting up HR system access on June 13, 2018.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

January 18, 2019

David P. Wheeler, ET 3C-K

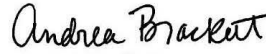
RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2018-15531 – HUMAN
RESOURCE SYSTEM PERSONALLY IDENTIFIABLE INFORMATION ACCESS
CONTROL

Our response to your request for comments regarding the subject draft report is
attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Melissa Conforti, and the audit team for their
professionalism and cooperation in conducting this audit. If you have any questions,
please contact Krystal Brandenburg or Scott Tiemeyer.



Wilson Taylor, III
Vice President, Ops Services & Ombudsman
Human Resources
WT 7D-K



Andrea Brackett
Chief Information Security Officer
Information Technology
WT 5D-K

ASB:SLW

cc (Attachment):

James Berrong, SP 3L-C
Krystal Brandenburg, MP 2B-C
Susan Collins, LP 6A-C
Trevor Cothron, SP 2A-C
Robertson Dickens, WT 9C-K
Jeremy Fisher, MP 3B-C
Megan Flynn, LP 3A-C
Denise Jones, WT 4A-K
Dwain Lanier, MR 6D-C

Todd McCarter, MP 2C-C
Jill Matthews, ET 4C-K
Philip Propes, SP 2A-C
Sherry Quirk, WT 7C-K
John Thomas III, MR 6D-C
Scott Tiemeyer, LP 3A-C
Diane Wear, WT 4B-K
OIG File No.2018-15531

AUDIT 2018-15531
Human Resource System PII Access Control
Response to Request for Comments

ATTACHMENT A
 Page 1 of 2

	Recommendation	Comments
1	We recommend the Director, TVA Cybersecurity: Implement a process to monitor the HR system for changes made by privileged users.	Management agrees. Both TVA Cybersecurity and HR have discussed this recommendation and believe the ownership should be reflected to be with HR. Management requests the recommendation clarify changes made by HR system administrators.
2	Ensure access reviews are consistently performed by the appropriate TVA managers and coordinated to involve the managers of those individuals with access to the application, as required by TVA-SPP-12.003, in conjunction with HR.	Management agrees. Both TVA Cybersecurity and HR have discussed this recommendation and believe the ownership should be reflected to be with HR. Management requests the recommendation clarify this is related to the administrator reviews of HR users with elevated access beyond self-service.
3	Complete the updated system authorization for the HR system as required by TVA-SPP-12.800.	The HR system was authorized 7/24/18 and documentation has been provided to the OIG.
4	Complete planned actions to document and fully implement the data loss prevention tool to monitor, detect, report, and notify when PII is shared electronically.	Management requests the Executive Summary (What the OIG Found), Draft Report (Findings pages 1 and 3) and Recommendation 4 clarify remediation is related to "agency restricted PII".
5	Review the NIST control gaps identified and determine the TVA policies that should be updated.	The NIST controls identified are documented in TVA's Consolidated Control Catalog and Enterprise Process Implementation documents and have been provided to the OIG.
6	We recommend the Vice President, HR Operations Services and Ombudsman: Update SOX documentation to include the access review process being performed, including a list to define appropriate managers to perform access reviews.	Management agrees.

AUDIT 2018-15531
Human Resource System PII Access Control
Response to Request for Comments

ATTACHMENT A
Page 2 of 2

	Recommendation	Comments
7	Remove the access for the two individuals identified who transferred and no longer have a need-to-know.	Management agrees and has remediated the access issues for the two identified individuals. Documentation has been provided to the OIG.