



Memorandum from the Office of the Inspector General

September 11, 2019

Jeremy P. Fisher, SP 3A-C
Todd M. Peney, WT 3C-K
Wilson Taylor III, WT 7D-K

REQUEST FOR MANAGEMENT DECISION – AUDIT 2019-15634 – TIMELY ACCESS REMOVAL

Due to potential risks associated with employee separations¹ where some Tennessee Valley Authority (TVA) employees ceased active work prior to their last official day of employment, we included an audit of timely access removal as part of our annual audit plan. Our audit objective was to determine if physical and logical access is removed when employees cease active work prior to retirement or other termination. Our scope included TVA employees whose employment ended during calendar year 2018 who ceased active work prior to retirement or other termination. We identified the employees as those with (1) more than 5 days between the last date worked and separation date (17 employees) and (2) employees with 70 or more hours of leave taken immediately prior to retirement or other separation (136 employees).

In summary, we found (1) TVA's policies and procedures do not provide guidance for supervisors/managers regarding removal of an employee's logical or physical access if they stop active work prior to separation, and (2) employee's physical and logical access is not consistently removed on a timely² basis when employees cease active work prior to retirement or other separation.

We recommend the Vice President, Human Resources (HR) Operations Services and Ombudsman, work with the Vice President and Chief Information Officer, Information Technology (IT), and the Director, TVA Police and Emergency Management to:

1. Develop guidance for supervisors/managers to notify TVA Cybersecurity and TVA Police and Emergency Management when an employee ceases active work prior to separation and include the period in which notification should be accomplished.
2. Develop a requirement for regular monitoring of physical and logical access removal when employees cease active work prior to separation.

¹ For the purposes of this report, we have used separation where possible at the request of TVA management, rather than termination. TVA's human resources system classifies all separations of service as "TER – termination," but TVA management believed the term would lead the reader to think of dismissals.

² Timely access removal was defined as logical and/or physical access to TVA assets removed within 7 days of the employee's last date worked. The 7-day criteria was based on North American Electric Reliability Corporation critical infrastructure protection regulatory requirements for individuals with unescorted (physical or logical) access to critical assets.

TVA management agreed with the recommendations in this report. See the Appendix for TVA management's complete response.

BACKGROUND

During calendar year 2018, 723 TVA employees ended employment with TVA. TVA has two primary Standard Programs and Processes (SPP) that address the removal of employees' logical and physical access:

- TVA-SPP-12.003, *IT Account Management*, establishes the process by which TVA will address the technical and procedural controls that enforce access authentication and authorization for both TVA account and non-TVA account activity on the TVA network.
- TVA-SPP-14.200, *Physical Access and Visitor Management*, establishes the agency's Physical Access and Visitor Management Program, which is designed to manage the physical access control systems for all facilities owned and leased by TVA and protect TVA's assets against unauthorized observation, removal, or manipulation.

The National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for federal systems. NIST Special Publication (SP) 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states, "Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access." Additionally, NIST states, "In general, organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions."

According to TVA Police and HR personnel, employees can have their logical and physical³ access removed automatically when the employee's HR status indicates the employee is no longer actively employed or manually removed upon management or other approved requests. The TVA Leader Handbook and HR Generalist Playbook state an employee's supervisor is responsible for notifying HR of all impending separations, including the anticipated separation date and type of separation as soon as notified.

TVA-SPP-14.200, *Physical Access and Visitor Management*, states physical access can be revoked when personnel with authorized physical access no longer have a business need to continue accessing a controlled area. Similar to the TVA Leader Handbook and HR Generalist Playbook, this SPP states it is the business unit manager's responsibility to notify TVA Access Control of any changes. Reasons for revoking access include, but are not limited to, completion of assigned task, changes to job description, reassignment to another position, extended absence, suspension, and termination of employment.

³ NIST defines physical access controls as controls that restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network server. NIST defines logical access controls as controls that explicitly enable or restrict the ability to do something with a computer resource (e.g., use, change, or view).

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if physical and logical access is removed when employees cease active work prior to retirement or other termination. The scope included TVA employees whose employment ended during calendar year 2018 who ceased active work prior to termination. To achieve our audit objective, we:

- Reviewed TVA-SPP-12.003, *IT Account Management*, to identify TVA's process for removing employees' logical access when they cease active work.
- Reviewed TVA-SPP-14.200, *Physical Access and Visitor Management*, to identify TVA's process for removing employees' physical access when they cease active work.
- Reviewed the TVA Leader Handbook to identify any guidance for supervisors/managers when an employee ceases active work prior to separation.
- Interviewed TVA personnel and reviewed program documentation, including TVA policies and procedures, to gain an understanding of TVA's process for removing employees' logical and physical access on a timely basis.
- Selected all employees whose employment ended during 2018 who ceased active work prior to separation. We identified the employees as those with (1) more than 5 days between the last date worked and separation date (17 employees) and (2) employees with 70 or more hours of leave taken immediately prior to retirement or other separation (136 employees).
- Reviewed logical and physical access records and separation data for the 153 employees by using 7 days between the employee's last date worked and the date their physical and/or logical access was removed to determine if access was removed timely.
- Reviewed NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, and the Institute of Internal Auditors Global Technology Audit Guide, *Identity and Access Management*, to identify best practices for management of logical access rights for employees who are leaving the organization.

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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS

We found (1) TVA's policies and procedures do not provide guidance for supervisors/managers regarding removal of an employee's logical or physical access if they stop active work prior to separation, and (2) employee's physical and logical access

is not consistently removed on a timely basis when employees cease active work prior to retirement or other separation.

LACK OF GUIDANCE FOR TIMELY ACCESS REMOVAL

We found the TVA Leader Handbook, TVA-SPP-12.003, *IT Account Management*, and TVA-SPP-14.200, *Physical Access and Visitor Management*, do not provide guidance to supervisors/managers to have an employee’s logical or physical access removed if they cease active work prior to separation. According to recommended practices issued by the Institute of Internal Auditors Global Technology Audit Guide, *Identity and Access Management*, policies should clearly identify what needs to happen when people leave the organization. Lack of guidance for timely access removal could lead to employees retaining logical access to TVA systems and physical access to TVA facilities (including buildings and data centers) after they have ceased active work.

LOGICAL AND PHYSICAL ACCESS IS NOT CONSISTENTLY REMOVED TIMELY

We found 68 (over 44 percent) of the 153 TVA employees who ceased active work prior to retirement or other separation during calendar year 2018 did not have logical and/or physical access to TVA assets removed on a timely basis. Table 1 shows the number of days between the last date worked and the date access was removed for the exceptions we identified. We found (1) 20 individuals maintained access after their last day worked to either TVA logical or physical assets, or both, for more than 90 days, (2) 9 individuals maintained access for 61-90 days, and (3) 12 individuals maintained access for 31-60 days.

Number of Days Between Last Date Worked and Access Removal Date					
Access Type	Number of Employees				Total
	8-30 Days	31-60 Days	61-90 Days	>90 Days	
Physical and Logical	12	9	9	13	43
Logical	13	3	0	5	21
Physical	2	0	0	2	4
Total	27	12	9	20	68

Table 1

NIST SP 800-14 states organizations should ensure effective administration of users’ computer access to maintain system security, and includes the following:

- Organizations should terminate system access as quickly as possible when an employee is leaving a position under terms they define as “less than friendly” given the potential for adverse consequences.
- If employees are to be fired, system access should be removed at the same time (or just before) the employees are notified of their dismissal.

- When an employee notifies an organization of a resignation and it can be reasonably expected it is on unfriendly terms, system access should be immediately terminated.

We found 6 of the individuals whose employment ended during 2018 left TVA under less than friendly terms. In addition, we found 33 of the individuals separated during 2018 resigned or left TVA due to a reduction-in-force. If management could reasonably expect these terms to be unfriendly, then access should have been removed immediately. Twenty of these individuals maintained some form of access to TVA assets for more than 30 days after their last date worked. The number of days lapsed between the last date worked and the removal of all access is shown in Table 2.

Days Between Last Date Worked and Access Removal	Discharged (Number of Employees)	Resigned / Reduction-in-Force (Number of Employees)
8 – 30 days	2	17
31 – 60 days	2	5
61 – 90 days	0	7
> 90 days	<u>2</u>	<u>4</u>
Total	6	33

Table 2

RECOMMENDATIONS

We recommend the Vice President, Human Resources Operations Services and Ombudsman, work with the Vice President and Chief Information Officer, IT, and the Director, TVA Police and Emergency Management to:

1. Develop guidance for supervisors/managers to notify TVA Cybersecurity and TVA Police and Emergency Management when an employee ceases active work prior to separation and include the period in which notification should be accomplished.
2. Develop a requirement for regular monitoring of physical and logical access removal when employees cease active work prior to separation.

TVA Management’s Comments – TVA management agreed with the recommendations in this report. See the Appendix for TVA management’s complete response.

- - - - -

Jeremy P. Fisher
Todd M. Peney
Wilson Taylor III
Page 6
September 11, 2019

This report is for your review and management decision. Please advise us of your management decision within 60 days from the date of this report. If you have any questions, please contact Michael C. Cook, Auditor, at (423) 785-4816 or Rick C. Underwood, Director, Financial and Operational Audits, at (423) 785-4824. 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

MCC:FAJ

cc: TVA Board of Directors
Clifford L. Beach, Jr., WT 7B-K
David L. Bowling, Jr., WT 11A-K
Andrea S. Brackett, WT 5D-K
Susan E. Collins, LP 6A-C
Robertson D. Dickens, WT 9C-K
Megan T. Flynn, LP 3A-C
Jeffrey J. Lyash, WT 7B-K
Todd E. McCarter, MP 2C-C
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Jack P. Paul, WT 2D-K
Sherry A. Quirk, WT 7C-K
Ronald R. Sanders II, MR 5E-C
Michael W. Sanford, WT 3C-K
Lisa D. Snyder, WT 3C-K
John M. Thomas III, MR 6D-C
OIG File No. 2019-15634

September 9, 2019

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2019-15634 – TIMELY
ACCESS REMOVAL

This is in response to your memorandum dated August 8, 2019. First, let me thank your team for the professional manner in which this audit was conducted. After review of the draft evaluation, please see the following response to the recommendations regarding Timely Access Removal.

RECOMMENDATIONS

We recommend the Vice President (VP) Human Resources Operations Services and Ombudsman, work with the Vice President and Chief Information Officer and the Director, TVA Police and Emergency Management (TVAP) to:

1. Develop guidance for supervisors/managers to notify TVA Cybersecurity and TVA Police and Emergency Management when an employee ceases active work prior to separation and include the period in which notification should be accomplished.

Response

Human Resources & Communications, Information Technology and TVAP Organizations are in agreement with the recommendation to develop guidance for supervisors/managers regarding timely removal of access prior to separation and active work.

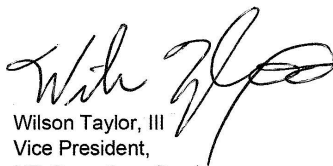
2. Develop requirement for regular monitoring of physical and logical access removal when employees cease active work prior to separation.

Response

Human Resources & Communications, Information Technology and TVAP Organizations are in agreement with the recommendation to develop a requirement for regular monitoring of physical and logical access removal when employees cease active work prior to separation.

David P. Wheeler
Page 2
September 9, 2019

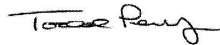
Thank you for allowing us to provide these comments. If you need additional information, please let us know.



Wilson Taylor, III
Vice President,
HR Operations Services
WT 7D-K



Jeremy P. Fisher
Vice President and
Chief Information Officer
SP 3A-C



Todd M. Peney
Director
TVAP and Emergency Management
WT 3C-K

cc: David Bowling, Jr., WT 11A-K
Clifford L. Beach, Jr., WT 7B-K
Andrea S. Brackett, WT 5D-K
Susan E. Collins, LP 6A-C
Robertson D. Dickens, WT 9C-K
Megan T. Flynn, LP 3A-C
Todd E. McCarter, MP 2C-C
Jack P. Paul, WT 2D-K
Sherry A. Quirk, WT 7C-K
Michael W. Sanford, WT 3C-K
Lisa D. Snyder, WT 3C-K
John M. Thomas III, MR 6D-C
OIG File No. 2019-15634