Memorandum from the Office of the Inspector General

October 21, 2020

Jeremy, P. Fisher
Todd M. Peney

REQUEST FOR MANAGEMENT DECISION – AUDIT 2020-15721 – INFORMATION TECHNOLOGY CONTRACTOR ACCESS

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 Weston J. Shepherd, Auditor, at (865) 633-7386 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)

WJS: KDS
Attachment
cc (Attachment):

TVA Board of Directors
David L. Bowling Jr.
Andrea S. Brackett
James R. Dalrymple
David Fountain
Benjamin A. Jones
Jeffrey J. Lyash
Justin C. Maierhofer
Jill M. Matthews
Todd E. McCarter
Jack P. Paul
Todd M. Peney
Sherry A. Quirk
Ronald R. Sanders
Michael W. Sanford
Michael D. Skaggs
Lisa D. Snyder
John M. Thomas III
Kay W. Whittenburg
OIG File No. 2020-15721

Office of the Inspector General

Audit Report

To the Vice President and Chief Information Officer, Information Technology, and to the Director, TVA Police and Emergency Management

INFORMATION TECHNOLOGY CONTRACTOR ACCESS

Audit Team
Weston J. Shepherd
Francis B. Lord II

Audit 2020-15721
October 21, 2020

ABBREVIATIONS

CIP	Critical Infrastructure Protected
IT	Information Technology
MT	Managed Task
NERC	North American Electric Reliability Corporation
SA	Staff Augmented
SPP	Standard Program and Process
TVA	Tennessee Valley Authority
TVAP	Tennessee Valley Authority Police

TABLE OF CONTENTS

APPENDIX

Audit 2020-15721 – Information Technology Contractor Access

EXECUTIVE SUMMARY

Why the OIG Did This Audit

Tennessee Valley Authority (TVA) Information Technology (IT) leadership announced in January 2020 to move toward a more contractor-based workforce. Subsequently, the Office of the Inspector General received multiple concerns that IT contractors with logical access did not have the necessary background investigation completed. Additionally, we previously conducted audits that found (1) insufficient TVA sensitive clearances for IT contractors whose job responsibilities required a sensitive clearance[i] and (2) issues with screening individuals prior to granting access to TVA systems.[ii] Subsequent to our fieldwork, in August 2020 TVA rescinded its previous decision to lay off IT workers in the move toward a more contractor-based workforce.

TVA IT and TVA Police require contractors have various levels of background investigations completed for logical access to different classifications of information. In addition, TVA requires all network users to complete cybersecurity awareness training on an annual basis.

Our objective was to determine if IT contractors are granted logical access in accordance with TVA policy. Our scope included onboarding actions completed for all active IT contractors as of March 26, 2020, including background investigations and cybersecurity awareness training requirements. Our scope did not include (1) nuclear clearance requirements for IT contractors, (2) the technical controls TVA has established to assign or manage logical access, or (3) review of National Security Clearances, as TVA does not conduct this level of screening for contractors.

What the OIG Found

We found that (1) TVA policy does not align between business units, (2) the majority of Tier 1 IT contractor suitability background investigations[iii] were not in accordance with TVA policy, and (3) the majority of IT contractor higher level background investigations[iv] were not in accordance with TVA policy. In addition, we found all the IT contractors with logical access included in our population of 326 had taken the annual cybersecurity awareness training in accordance with TVA policy.

---

[i] Audit 2010-13132 *Review of Physical and Logical Access for Contractors*, June 15, 2011.

[ii] Audit 2019-15653 *Federal Information Security Modernization Act*, February 12, 2020.

[iii] Tier 1 suitability investigations are for nonsensitive government positions.

[iv] For the purposes of this audit, higher level background investigations include background investigations for Tier 2 moderate risk public trust positions and/or logical access to North American Electric Reliability Corporation Critical Infrastructure Protected assets.

Audit 2020-15721 – Information Technology Contractor Access

EXECUTIVE SUMMARY

What the OIG Recommends

We recommend the Vice President and Chief Information Officer, IT, and the Director, TVA Police and Emergency Management:

1. Review and update TVA policies to clarify background investigation requirements and ensure alignment between business units.

2. Develop a process to implement requirements for logical access and ensure IT contractors have the required Tier 1 background investigation in a timely manner.

3. Develop a process to implement requirements for logical access, including administrative access, and ensure IT contractors have the required higher level background investigation in a timely manner.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with the recommendations in this report. In addition, TVA management stated (1) the updated policies need additional clarifying language, (2) most contractors were granted physical access and vetted by TVA Police prior to allowing logical access, and (3) the assessed risk of insider threat to be low. See the Appendix for TVA management's complete response.

Auditor's Response

Prior to receiving TVA's response to our draft audit report, we had discussions with TVA management regarding clarification of (1) types of background investigations, (2) National Security Clearances, (3) North American Electric Reliability Corporation Critical Infrastructure Protected requirements, and (4) the "equivalent" phrase in TVA IT policy, and revised our report accordingly. Based on discussions with TVA management and their comments in the Appendix, we revised (1) recommendation 1 to include updating TVA policies to clarify background investigation requirements and (2) the report to more accurately describe the risk of a potential insider threat incident.

BACKGROUND

Tennessee Valley Authority (TVA) Information Technology (IT) leadership announced in January 2020 a decision to move toward a more contractor-based workforce. Subsequently, the Office of the Inspector General received multiple concerns that IT contractors with logical access did not have the necessary background investigation completed. Additionally, we previously conducted audits that found (1) insufficient TVA sensitive clearances for IT contractors whose job responsibilities required a sensitive clearance[1] and (2) issues with screening individuals prior to granting access to TVA systems.[2] Subsequent to our fieldwork, in August 2020 TVA rescinded its previous decision to lay off IT workers in the move toward a more contractor-based workforce.

TVA IT and TVA Police (TVAP) require contractors have various levels of background investigations completed for logical access to different classifications of information. Table 1 shows the levels of background investigations that TVA conducts for contractors:

Types of Contractor Background Investigations	Description	TVA Applicability
Tier 1	Suitability investigation for nonsensitive government positions.	Conducted by TVAP for TVA employees and staff augmented contractors.
Tier 2	Additional background investigation to determine eligibility for moderate risk public trust positions.	According to TVA personnel, TVAP granted Tier 2 TVA Sensitive security clearance to individuals with access to TVA designated sensitive information prior to September 28, 2018. This has since been updated to align with federal level Tier 2 investigations, and conducted as requested by TVA managers and supervisors. As reinvestigations occur for individuals granted this clearance prior to the alignment, they are granted the federal level Tier 2 eligibility.
North American Electric Reliability Corporation (NERC) Critical Infrastructure Protected (CIP)	Investigation required for individuals with authorized logical access to NERC CIP assets.	Conducted by TVAP as requested by TVA managers and supervisors.

Table 1

Although the Tier 2 background and NERC CIP investigations are referred to as security clearances in TVA policy, they are not considered National Security Clearances.[3]

[1] Audit 2010-13132 *Review of Physical and Logical Access for Contractors*, June 15, 2011.

[2] Audit 2019-15653 *Federal Information Security Modernization Act*, February 12, 2020.

[3] According to the *Federal Investigative Standards Crosswalk Job Aid*, only Tier 3 and Tier 5 Investigations are referred to as Security Clearances. <https://www.dhs.gov/sites/default/files/publications /federal_investigative_standards_crosswalk_guide.pdf>, accessed on July 16, 2020.

TVA hires three types of contractors—staff augmented (SA), managed task (MT), and consultant—that are distinguished by the nature of supervision and type of assignment. TVA's Standard Program and Process (SPP) 11.106, *Contingent Labor Onboarding and Offboarding*, defines these as:

- SA Contractor – contractors who temporarily supplement the TVA workforce and are under the supervision of a TVA employee.
- MT Contractor – contractors who are managed by a supplier providing services to TVA as defined or agreed to by TVA.
- Consultant – an individual or firm hired to provide independent advice and expertise.

On March 26, 2020, TVA had 326 IT contractors with logical access. The IT contractors consisted of:

- SA Contractors – 182
- MT Contractors – 140
- Consultants – 4

Chart 1 below shows the timeframe in which the IT contractors were hired at TVA.

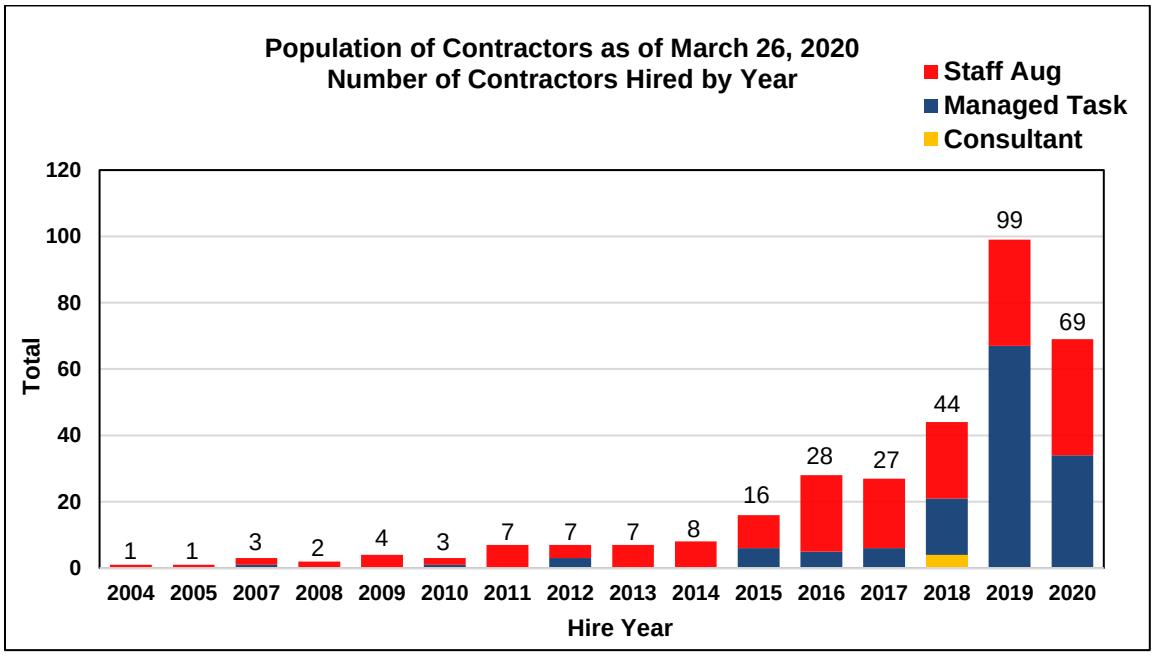

Chart 1

The 326 IT contractors had hire dates ranging from 2004 to 2020.

TVA has designated three classifications of information based on sensitivity that are more sensitive than public information. TVA-SPP-12.002, *TVA Information Management Policy*, requires that individuals with logical access to information

more sensitive than public information must have a Tier 1 employee suitability investigation or equivalent or a higher level background investigation. TVA-SPP-14.440, *Contractor Fitness*, requires that (1) SA contractors are required to have a contractor Tier 1 suitability investigation or higher level clearance and (2) consultants and MT contractors are required to have a minimum of a fingerprint check for Federal Bureau of Investigation criminal history. In addition, TVA-SPP-14.430, *Security Clearances*, requires that (1) contractors with access to TVA designated sensitive information require a Tier 2 background investigation that needs to be renewed every 5 years, and (2) contractors with authorized logical access to NERC CIP assets require a NERC clearance that needs to be renewed every 7 years.

In addition, TVA requires all network users to complete cybersecurity awareness training on an annual basis. TVA-SPP-12.017, *Security Awareness and Training*, requires that users take a cybersecurity training prior to being granted logical access and is conducted on an annual basis.

We performed this audit due to the concerns our office received on IT contractor logical access without proper background investigation and screening issues noted on previous audits. Prior to receiving TVA's comments on our draft audit report, we had discussions with TVA management regarding clarification of (1) types of background investigations, (2) National Security Clearances, (3) NERC CIP requirements, and (4) the "equivalent" phrase in TVA IT policy, and revised our report accordingly.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if IT contractors are granted logical access in accordance with TVA policy. Our scope included onboarding actions completed for all 326 active IT contractors as of March 26, 2020, including background investigations and cybersecurity awareness training requirements. Our scope did not include (1) nuclear clearance requirements for IT contractors, (2) the technical controls TVA has established to assign or manage logical access or (3) review of National Security Clearances, as TVA does not conduct this level of screening for contractors. Our fieldwork was performed between March 2020 and July 2020. As a result, our findings do not represent any process changes that have been implemented or the status of IT contractors hired after March 26, 2020.

To achieve our objective, we:

- Reviewed applicable TVA SPPs to obtain an understanding of TVA's contractor process and screening requirements, including:
  - TVA-SPP-11.106, *Contingent Labor Onboarding and Offboarding*
  - TVA-SPP-12.002, *TVA Information Management Policy*
  - TVA-SPP-12.017, *Security Awareness and Training*
  - TVA-SPP-14.200, *Physical Access and Visitor Management*
  - TVA-SPP-14.420, *Employment Suitability*
  - TVA-SPP-14.430, *Security Clearances*
  - TVA-SPP-14.440, *Contractor Fitness*
- Obtained employment records and a listing of users with logical access to identify the IT contractor population as of March 26, 2020.
- Obtained IT contractor background investigation records from TVA's human resource system.
- Compared IT contractor background investigation records to TVA requirements to determine if IT contractors met the requirements.
- Judgmentally selected 5 of 33 IT personnel contract vendors that provided approximately 71 percent of the IT contractors with logical access as of March 26, 2020. We reviewed the contracts' terms and conditions to determine if the contracts required vendors to perform any screening for their employees. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Reviewed IT contractor's logical access to systems that require a Tier 2 background investigation to determine if the IT contractors met those requirements.
- Reviewed IT contractor's logical access roles and compared them to logical access role requirements to determine if the IT contractors met the background investigation requirements identified for the roles.
- Reviewed training records to determine if the IT contractors had taken annual cybersecurity awareness training as required by TVA policy.
- Obtained an understanding of internal controls associated with the contractor background investigation process and annual cybersecurity training requirements. We identified these controls as significant to the audit objective and included them in our audit testing.

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 AND RECOMMENDATIONS

In summary, we found that (1) TVA policy does not align between business units, (2) the majority of Tier 1 IT contractor suitability background investigations were not in accordance with TVA policy, and (3) the majority of IT contractor higher level background investigations[4] were not in accordance with TVA policy. In addition, we found all the IT contractors with logical access included in our population of 326 had taken the annual cybersecurity awareness training in accordance with TVA-SPP-12.017, *Security Awareness and Training*.

TVA POLICY DOES NOT ALIGN BETWEEN BUSINESS UNITS

TVA has defined background investigation requirements; however, the requirements documented in TVA IT and TVAP policies do not align. TVA IT and TVAP policy requirements are outlined in Table 2:

TVAP Requirements – TVA-SPP-14.440, *Contractor Fitness*	**TVA IT Requirements – TVA-SPP-12.002, *TVA Information Management Policy***
SA contractors are required to have a contractor suitability investigation or higher level clearance[5].	Individuals with logical access to information more sensitive than public information have employee suitability or equivalent or a higher level clearance[6].
Consultants and MT contractors are required to have a minimum of a fingerprint check for FBI criminal history.	

Table 2

As shown in Table 2, TVA IT policy (TVA-SPP-12.002) requires a Tier 1 suitability investigation or equivalent or higher level clearance for all individuals with logical access to information more sensitive than public information; however, TVAP policy (TVA SPP-14.440) does not require a Tier 1 background investigation for consultants or MT contractors with logical access.

In addition, TVA IT policy (TVA-SPP-12.002) allows an equivalent to employee suitability, but does not define what would be an equivalent. According to TVA IT personnel, an equivalent level of screening would include any screening conducted by a contract vendor or TVAP. However, according to TVAP personnel, there is no equivalent for a Tier 1 background investigation.

The inconsistencies in requirements in TVA IT and TVAP policies can lead to individuals not having the proper background investigation.

Recommendation – We recommend the Vice President and Chief Information Officer, IT, and the Director, TVAP and Emergency Management, review and

[4] For the purposes of this audit, higher level background investigations include background investigations for Tier 2 moderate risk public trust positions and/or logical access to NERC CIP assets.

[5] Higher level background investigation is defined by TVAP personnel as a Tier 2 background investigation or higher, and does not include a NERC CIP background investigation.

[6] Higher level background investigation is defined by TVA IT personnel as a Tier 2 background investigation or higher, which includes a NERC CIP background investigation.

update TVA policies to clarify background investigation requirements and ensure alignment between business units.

TVA Management's Comments – TVA management agreed with the recommendation and stated the updated policies need additional clarifying language. See the Appendix for TVA management's complete response.

Auditor's Response – Based on discussions with TVA management and their comments in the Appendix, we revised our recommendation to include updating TVA policies to clarify background investigation requirements.

MAJORITY OF TIER 1 IT CONTRACTOR SUITABILITY BACKGROUND INVESTIGATIONS WERE NOT IN ACCORDANCE WITH TVA POLICY

We reviewed records from TVA's human resource system related to background investigations for the 326 IT contractors with logical access as of March 26, 2020, for compliance with both TVA policies mentioned above. We found 171 of the 326 (52 percent) IT contractors were not in compliance with the TVAP policy background investigation requirements. Specifically, the 171 were either (1) SA contractors with no active Tier 1 or higher level background investigation, or (2) consultants or MT contractors with no fingerprint record or higher level background investigation as required by TVA-SPP-14.440. We also found 246 of the 326 (75 percent) IT contractors did not have active Tier 1 or higher level background investigation as required by TVA IT Policy (TVA-SPP-12.002). We determined that neither TVA-SPP-12.002 nor TVA-SPP-14.440 defined timing requirements for completing background investigations.

According to TVAP personnel, the reasons for the noncompliance with TVA policies included:

- Some IT contractors were hired prior to a TVAP policy change on June 12, 2017, that introduced additional requirements for SA contractors to have a Tier 1 background investigation or higher level background investigation.
- Some IT contractors had a Tier 1 case in progress.
- Some IT contractors had a higher level background investigation case in progress.

Table 3 on the following page shows the timeframe in which the IT contractors who were not in accordance with TVA policies were hired at TVA.

Hire Year	Not in Accordance with TVAP Policy (TVA-SPP-14.440)	Not in Accordance with TVA IT Policy (TVA-SPP-12.002)	Total Number of IT Contractors with Logical Access
2004	1	1	1
2005	1	1	1
2007	0	1	3
2008	1	1	2
2009	2	1	4
2010	0	0	3
2011	3	3	7
2012	2	3	7
2013	3	2	7
2014	4	4	8
2015	7	9	16
2016	14	13	28
2017	14	16	27
2018	17	35	44
2019	54	89	99
2020	48	67	69
Totals	**171**	**246**	**326**

Table 3

TVA has a potential risk of an insider threat incident due to granting IT contractors logical access without having the required background investigations.

Recommendation – We recommend the Vice President and Chief Information Officer, IT, and the Director, TVAP and Emergency Management, develop a process to implement requirements for logical access and ensure IT contractors have the required Tier 1 background investigation in a timely manner.

TVA Management's Comments – In response to our draft report, TVA management stated they agree with the recommendation. Additionally, TVA management stated that (1) most contractors were granted physical access and vetted by TVAP prior to allowing logical access and (2) based on the existence of compensating controls, the assessed risk of insider threat is low. See the Appendix for TVA management's complete response.

Auditor's Response – We did not consider granting physical access to be compliant with the TVA IT policy, as this was not specified as an equivalent screening for granting logical access. As a result, we determined 75 percent noncompliance with IT policy. Regarding the characterization of an increased insider threat risk, based on TVA management's comments, the report was updated to more accurately describe the risk of a potential insider threat incident.

MAJORITY OF IT CONTRACTOR HIGHER LEVEL BACKGROUND INVESTIGATIONS WERE NOT IN ACCORDANCE WITH TVA POLICY

According to TVA-SPP-14.430, *Security Clearances*, TVA managers and supervisors are responsible for requesting Tier 2 background investigations for employees and contractors when needed. We reviewed background investigation records from TVA's human resource system for IT contractors with logical access as of March 26, 2020, and identified 73 IT contractors with TVA requirements for Tier 2 background investigations based on their logical access roles. We found 49 of the 73 (67 percent) did not have the required Tier 2 background investigation based on their logical access roles. TVAP informed us the TVA manager or supervisor had not requested the required Tier 2 background investigation for 43 of these 49 IT contractors.

In addition, we identified 19 IT contractors with administrative access to systems that require Tier 2 background investigation. We found 3 of the 19 (16 percent) IT contractors with administrative access did not have the required Tier 2 background investigation. TVAP informed us that the TVA manager or supervisor had not requested the required Tier 2 background investigation for 2 of these 3 IT contractors.

TVA has a potential risk of an insider threat incident due to granting IT contractors logical access without having the required background investigation.

Recommendation – We recommend the Vice President and Chief Information Officer, IT, and the Director, TVAP and Emergency Management, develop a process to implement requirements for logical access, including administrative access, and ensure IT contractors have the required higher level background investigation in a timely manner.

TVA Management's Comments – In response to our draft report, TVA management agreed with our recommendation. Additionally, TVA management stated that based on the existence of compensating controls, the assessed risk of insider threat is low. TVA management also asserted that all IT employees and contractors with the need for a NERC CIP clearance are appropriately cleared for and meet the NERC CIP requirements. See the Appendix for TVA management's complete response.

Auditor's Response – Based on TVA management's comments on increased risk, the report was updated to more accurately describe the risk of a potential insider threat incident.

September 30, 2020

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2020-15721 – INFORMATION TECHNOLOGY CONTRACTOR ACCESS

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, Weston Shepherd, and the audit team for their professionalism and cooperation in conducting this audit. We appreciate the Office of the Inspector General's role to audit our processes and help identify opportunities for improvement. If you have any questions, please contact Brandy Brown or Jack Paul.

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

Todd Peney
Director, TVA Police and Emergency Management
WT 3C-K

ASB: BAB
cc (Attachment): Response to Request
David Bowling, WT 11A-K
Samuel Austin, MP 3B-C
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
James Dalrymple, MR 3H-C
David Harrison, MP 5C-C
Benjamin Jones, SP 3L-C
Jeffrey Lyash, WT 7B-K
Jill Matthews, WT 2C-K
Todd McCarter, MP 2C-C
Jack Paul, WT 2D-K
Sherry Quirk, WT 7C-K
Tricia Roelofs, WT 6A-K
Ronald Sanders, MR 5E-C
Michael Sanford, WT 3C-K
Michael Skaggs, WT 7B-K
Lisa Snyder, WT 3C-K
John Thomas, MR 6D-C
OIG File No. 2020-15721

Audit 2020-15721
Information Technology Contractor Access
Response to Request for Comments

Page	Draft Report Section	Comments
	All	TVA takes its responsibility for information security and infrastructure reliability seriously. Multiple layers of both physical, logical and administrative controls are in place to provide highly redundant protection for vital information and control systems. While the scope of the audit excluded these controls as a part of this effort, it is important that these practices are considered in order to have a fully-informed, comprehensive, view of the processes required to obtain access to various systems. TVA recognized inconsistency in our contractor vetting processes and initiated an internal, collaborative effort to address those issues prior to the initiation of the audit. These efforts will continue in order to ensure a consistent approach for background investigations and granting of physical and logical access. As stated by the OIG in this report, in August 2020 TVA announced the cancellation of contracts which would have displaced IT workers and increased contractor usage. We will continue to move to an employee-based approach to deliver IT services across TVA.

Recommendation		Comments
1	We recommend the Vice President and Chief Information Officer, IT, and the Director, TVA Police and Emergency Management: Review and update TVA policies to ensure alignment of screening requirements between business units.	Management agrees with the recommendation and would add updated policies need to clarify the language and intent of the screenings and access processes across business units as well as the expectations of TVA managers in complying with the processes.

Audit 2020-15721
Information Technology Contractor Access
Response to Request for Comments

ATTACHMENT A
Page 2 of 1

Recommendation		Comments
2	Develop a process to implement screening requirements for logical access and ensure IT contractors have the required Tier 1 background investigation in a timely manner.	Management agrees with the recommendation but would stipulate that most contractors were granted physical access and vetted by TVAP prior to allowing logical access. This is in alignment with the "equivalent" logical access vetting process stated in the IT policy. Additonally, because sufficient compensating controls are in place, TVA assesses the increased potential risk of insider threat to be low. As stated in the audit scope, this evaluation did not include various compensating controls within the IT work processes. IT has full audit attribution of actions taken by IT personnel and monitors for activity outside of approved work processes. As the final compensating control, the TVA insider threat program reduces the risk of insider threat. This program is in place to detect inappropriate actions by all personnel.
3	Develop a process to implement requirements for logical access, including administrative access, and ensure IT contractors have the required higher level background investigation in a timely manner.	Management agrees with the recommendation in regards to the Tier 2 investigations for "sensitive" related logical access. TVA asserts all IT employees and contractors with the need for a NERC CIP clearance are appropriately cleared for and meet the NERC CIP regulatory requirements. As with the second recommendation, TVA assesses the increased potential risk of insider threat to be low, again citing the existance of compensating controls which was explicitly excluded from this audit activity.