Memorandum from the Office of the Inspector General

April 29, 2020

Jeremy P. Fisher
Todd M. Peney

REQUEST FOR MANAGEMENT DECISION – AUDIT 2019-15619 – INSIDER THREAT PROGRAM

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

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

MLC:KDS
Attachment
cc (Attachment):

TVA Board of Directors
David L. Bowling Jr.
Andrea S. Brackett
Erin L. Cole
Kelie H. Hammond
Jeffrey J. Lyash
Justin C. Maierhofer
Todd E. McCarter
Jill M. Matthews
Jack P. Paul
Sherry A. Quirk
Ronald R. Sanders II
Michael W. Sanford
Michael D. Skaggs
Lisa D. Snyder
John M. Thomas III
OIG File No. 2019-15619

Office of the Inspector General

Audit Report

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

INSIDER THREAT PROGRAM

Audit Team
Melissa L. Conforti
Megan E. Spitzer

Audit 2019-15619
April 29, 2020

SYNOPSIS

We included an audit of Tennessee Valley Authority's (TVA) Insider Threat Program (ITP) as part of our annual audit plan due to potential risks associated with insider threats, including espionage, sabotage, intellectual property theft, fraud, and violence. In January 2019, we were informed TVA was developing a Standard Programs and Processes (SPP) to govern a formal ITP. TVA chose to implement their ITP agency wide to protect TVA personnel, facilities, information systems, and the information within such systems. In February 2020, TVA-SPP-14.120, *Insider Threat Program*, was developed and approved by TVA management with an effective date planned for April 1, 2020. Subsequent to our draft report, TVA management informed us the planned effective date had been changed to July 1, 2020.

Our audit objective was to determine if TVA had a program established to address insider threats that was consistent with best practices. Our scope was limited to the current state of TVA's ITP. Our fieldwork was performed from June 2019 through February 2020.

We found several areas where TVA's ITP was consistent with best practices. Additionally, TVA had designated a senior official charged with overseeing classified information sharing and safeguarding efforts of the agency. Although TVA had not yet implemented its planned ITP, we determined TVA's program will be at a proactive maturity level upon its implementation. Also, we identified best practices that were not currently included in the developed ITP related to monitoring and awareness training.

We made five specific recommendations to TVA management to implement the ITP and incorporate best practices related to monitoring and training. Our specific recommendations are included within the report.

TVA Management's Comments – TVA management agreed with the recommendations in this report. See Appendix C 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 in (1) the planned implementation date for the developed ITP and (2) the best practice considerations finding section and revised our report accordingly.

BACKGROUND

Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, was released in October 2011. The EO charged an interagency insider threat task force, known as the National Insider Threat Task Force (NITTF), to develop a government-wide program for deterring, detecting, and mitigating insider threats. This program included the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. Specifically, the EO requires agencies to:

- Designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts of the agency.
- Implement an insider threat detection and prevention program consistent with guidance and standards developed by the NITTF.
- Perform self-assessments of compliance with policies and standards and report annually to a federal steering committee.
- Provide information and access as warranted and consistent with law to enable independent assessments by the federal government and the NITTF.
- Assign staff as appropriate and necessary to the federal government and the NITTF on an ongoing basis.

TVA-SPP-14.380, *Classified National Security Information*, implemented the applicable requirements in various EOs and regulations including EO 13587*.* This SPP requires TVA establishment, implementation, monitoring, and reporting on the effectiveness of its Insider Threat Detection and Prevention Program.

While EO 13587 was specifically related to protecting classified information, TVA chose to implement an ITP agency wide to protect TVA personnel, facilities, information systems, and the information within such systems. In January 2019, we were informed TVA was developing an SPP to govern a formal ITP to be implemented by March 2019. In June 2019, we began our audit with the understanding that TVA was still developing the SPP. In February 2020, TVA-SPP-14.120, *Insider Threat Program,* was approved with an effective date planned for April 1, 2020. Subsequent to our draft report, TVA management informed us the planned effective date had been changed to July 1, 2020. The SPP establishes controls to prevent espionage, violent acts against TVA, and unauthorized access or misuse of TVA information and information systems by deterring employees from becoming insider threats and detecting active threats.

As part of our annual audit plan, we completed a threat assessment to identify high-risk cybersecurity threats that could potentially impact TVA. Therefore, we included an audit of TVA’s ITP in our annual audit plan.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if TVA had a program established to address insider threats that was consistent with best practices. Our scope was limited to the current state of TVA's ITP. Our fieldwork was performed from June 2019 through February 2020. A complete discussion of our audit objective, scope, and methodology is included in Appendix A.

FINDINGS

We found several areas where TVA's ITP was consistent with best practices. Specifically, TVA:

- Utilized the NITTF *Insider Threat Maturity Model* for their implementation plan.
- Assigned business unit representation in the ITP development team meetings and taskforce that followed the Department of Defense insider threat best practices.[1]
- Training for the ITP development team and taskforce followed the Center for Development of Security Excellence's ITP best practices.[2]

Additionally, TVA designated a senior official charged with overseeing classified information sharing and safeguarding efforts of the agency, including the ITP.

Although TVA had not yet implemented its planned ITP, we determined TVA's program will be at a proactive maturity level upon its implementation. Also, we identified best practices that were not currently included in the developed ITP related to monitoring and training. Details of our findings are discussed below.

INSIDER THREAT PROGRAM NOT IMPLEMENTED

TVA-SPP-14.120, *Insider Threat Program*, was developed and approved by TVA management during our audit; however, it has not been implemented. Additionally, the TVA *Insider Threat Program Operational Support Plan* was developed; however, it has not been finalized or implemented. In February 2020, TVA-SPP-14.120, *Insider Threat Program*, was developed and approved by TVA management with an effective date planned for April 1, 2020. Subsequent to our draft report, TVA management informed us the planned effective date had been changed to July 1, 2020.

Although the SPP and the TVA *Insider Threat Program Operational Support Plan* have not been implemented, we reviewed the developed documents to assess the ITP maturity. The *2019 Insider Threat Program Maturity Model Report* was created to help security professionals assess their organization's ability to monitor for, detect, and respond to insider threats. Using the *2019 Insider Threat Program Maturity Model Report*, we determined TVA's overall ITP maturity level to be proactive. See Appendix B for details on the maturity levels. As shown in Table 1 on the following page, a proactive ITP includes a focus on the use of technologies and interdepartmental communication that will help spot any insider threats.

[1] The best practice recommends including personnel from human resources, security, Information Technology (IT), equal opportunity, general counsel, and counterintelligence that provide subject matter expert support as needed.

[2] The best practice includes utilization of the NITTF's training materials.

Maturity Level	Definition
Nonexistent	The organization has no program or technology in place to detect and respond to insider threats and is unaware of the risk posed by an insider threat.
Reactive	The organization has no program in place but is aware that insider threats exist. IT is responsible for responding to any realized threat actions.
Proactive	The organization's focus is on the use of technologies (and the necessary interdepartmental communication to facilitate use) that will help spot any insider threats within a core group of high-risk users.
Predictive	The organization has a formal program in place that seeks to identify potential or active threats as early as possible. Program definitions, policies, processes, and technologies are in place organization wide.
Optimized	The organization's program is holistic, dynamic, and responsive, continually addressing shifting risk and changes in business operations that impact needed policy, process, and technologies.

Table 1

Specifically, as shown in Table 2, we determined TVA's ITP had maturity levels for each of the maturity sections ranging from reactive to optimized based on our analysis of the maturity sections and associated maturity level definitions.

Maturity Section	Assessed Maturity Level
Goals and Objectives	Reactive
Awareness	Reactive
Governance	Predictive
Risk Assessment	Proactive
Policies	Predictive
Monitoring	Proactive
Processes	Proactive
Intelligence Sources	Proactive
Communications and Training	Optimized

Table 2

See Appendix B for details on the metrics for the maturity sections.

BEST PRACTICE CONSIDERATIONS

We identified best practices that were not currently included in the planned TVA-SPP-14.120, *Insider Threat Program* and the draft *Insider Threat Program Operational Support Plan* related to (1) monitoring network and user activity and (2) awareness training.

Monitoring

We identified best practices that were not included in the planned TVA-SPP-14.120, *Insider Threat Program* and the draft *Insider Threat Program Operational Support Plan* related to monitoring network and user activity.

Specifically, TVA's planned ITP does not include (1) baselining[3] normal user activity on the network to establish trends and (2) monitoring account activity of personnel with access to high-risk systems and/or facilities for a defined period of time when they leave the organization.

The Office of the Inspector General performed an audit[4] regarding the timely removal of access in 2019. The audit found employees logical and physical access was not consistently removed on a timely basis when employees ceased active work prior to retirement or separation. The risk of employees retaining access after they have ceased work increases the need to (1) monitor personnel before and after they terminate and (2) baseline personnel activity to identify potential insider threats.

Awareness Training

We identified best practices that were not included in the developed ITP related to awareness training. TVA's training for personnel holding a clearance does not include (1) the importance of detection and reporting potential threats to proper authorities, (2) methods used by adversaries to recruit insiders and/or collect information, and (3) counterintelligence and security reporting requirements. This is a best practice recommended by the Center for Development of Security Excellence's "Establishing an Insider Threat Program for Your Organization."[5] Also, TVA's ITP does not currently reward employees spotted doing something good for security, which is recommended by Software Engineering Institute's "Common Sense Guide to Mitigating Insider Threats."[6] Robust training and reporting procedures promote personnel awareness of detecting and deterring malicious and unintentional insider threats.

RECOMMENDATIONS

We recommend the Director, TVA Police and Emergency Management:

1. Continue planned implementation of the ITP, including TVA-SPP-14.120, *Insider Threat Program*, and the TVA *Insider Threat Program Operational Support Plan*.

2. Implement and incorporate a formal positive reward program into TVA's ITP.

[3] Baselines are a minimum or a starting point for comparison.

[4] Audit Report 2019-15634, *Timely Access Removal*, September 11, 2019.

[5] "Establishing an Insider Threat Program for Your Organization," July 2013, <https://www.cdse.edu/documents/student-guides/INT122-guide.pdf>, accessed on June 25, 2019.

[6] Carnegie Mellon University, Software Engineering Institute, "Common Sense Guide to Mitigating Insider Threats," Sixth Edition, December 2018.

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

3. Incorporate monitoring into TVA's ITP to include personnel with access to high-risk systems and/or facilities for a period of time when they terminate employment.

4. Incorporate baselining of normal user activity on the network for access to high-risk systems and/or facilities into TVA's ITP.

5. Incorporate the importance of (1) detection and reporting potential threats to proper authorities, (2) methods used by adversaries to recruit insiders and/or collect information, and (3) counterintelligence and security reporting requirements into the annual Cybersecurity Awareness training.

TVA Management's Comments – TVA management agreed with our recommendations in this report. See Appendix C 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 in (1) the planned implementation date for the developed ITP and (2) the best practice considerations finding section and revised our report accordingly.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if Tennessee Valley Authority (TVA) had a program established to address insider threats that was consistent with best practices. Our scope was limited to the current state of TVA's Insider Threat Program (ITP). Our fieldwork was performed from June 2019 through February 2020. To achieve our objective, we:

- Reviewed applicable TVA Standard Programs and Processes (SPP), Work Instruction (WI) and other guidance to gain an understanding of TVA's processes related to insider threats, including:
  - Draft TVA *Insider Threat Program Operational Support Plan*
  - TVA-SPP-14.120, *Insider Threat Program*[1]
  - TVA-SPP-14.380, *Classified National Security Information*
  - TVA-SPP-12.001, *Acceptable Use of Information Resources*
  - TVA-SPP-14.200, *Physical Access and Visitor Management*
  - IT-WI-12.05.002, *Enterprise Security Monitoring Services – Catalog Service Request Submission Instructions*
  - "TVA Code of Conduct"
- Reviewed TVA training content, including TVA's annual cybersecurity awareness, National Clearance Holders Training, and ITP Training for those with ITP roles and responsibilities to determine if best practices were included.
- Observed ITP development team meetings from June 2019 through February 2020, including a walkthrough of an ITP scenario utilizing the Insider Threat System on January 8, 2020.
- Obtained and reviewed Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011.
- Identified applicable insider threat best practices and performed a gap analysis of TVA policies, procedures, and documents addressing the ITP, including:
  - Software Engineering Institute's "Common Sense Guide to Mitigating Insider Threats"[2]
  - "Global Technology Audit Guide" Auditing Insider Threat Programs[3]

[1] This SPP has a planned effective date of July 1, 2020.

[2] Carnegie Mellon University, Software Engineering Institute, "Common Sense Guide to Mitigating Insider Threats," Sixth Edition, December 2018.

[3] The Institute of Internal Auditors, Inc., "Global Technology Audit Guide," Auditing Insider Threat Programs, August 14, 2018.

  - Center for Development of Security Excellence's "Establishing an Insider Threat Program for Your Organization"[4]
  - Department of Defense's "Insider Threat Program – Best Practices – Hub Hiring"[5]

- Reviewed the *2019 Insider Threat Program Maturity Model Report* and determined TVA's program maturity using defined metrics for each maturity section. We determined the overall ITP maturity level by using the simple majority rule of the most frequent resulting maturity levels for each maturity section. See Appendix B for details on the maturity model.
- Inquired with TVA personnel to gain an understanding of TVA's ITP.

We did not identify internal controls significant to our audit objectives; therefore, internal controls were not tested as part of this audit. 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.

[4] "Establishing an Insider Threat Program for Your Organization," July 2013, <https://www.cdse.edu/documents/student-guides/INT122-guide.pdf>, accessed on June 25, 2019.

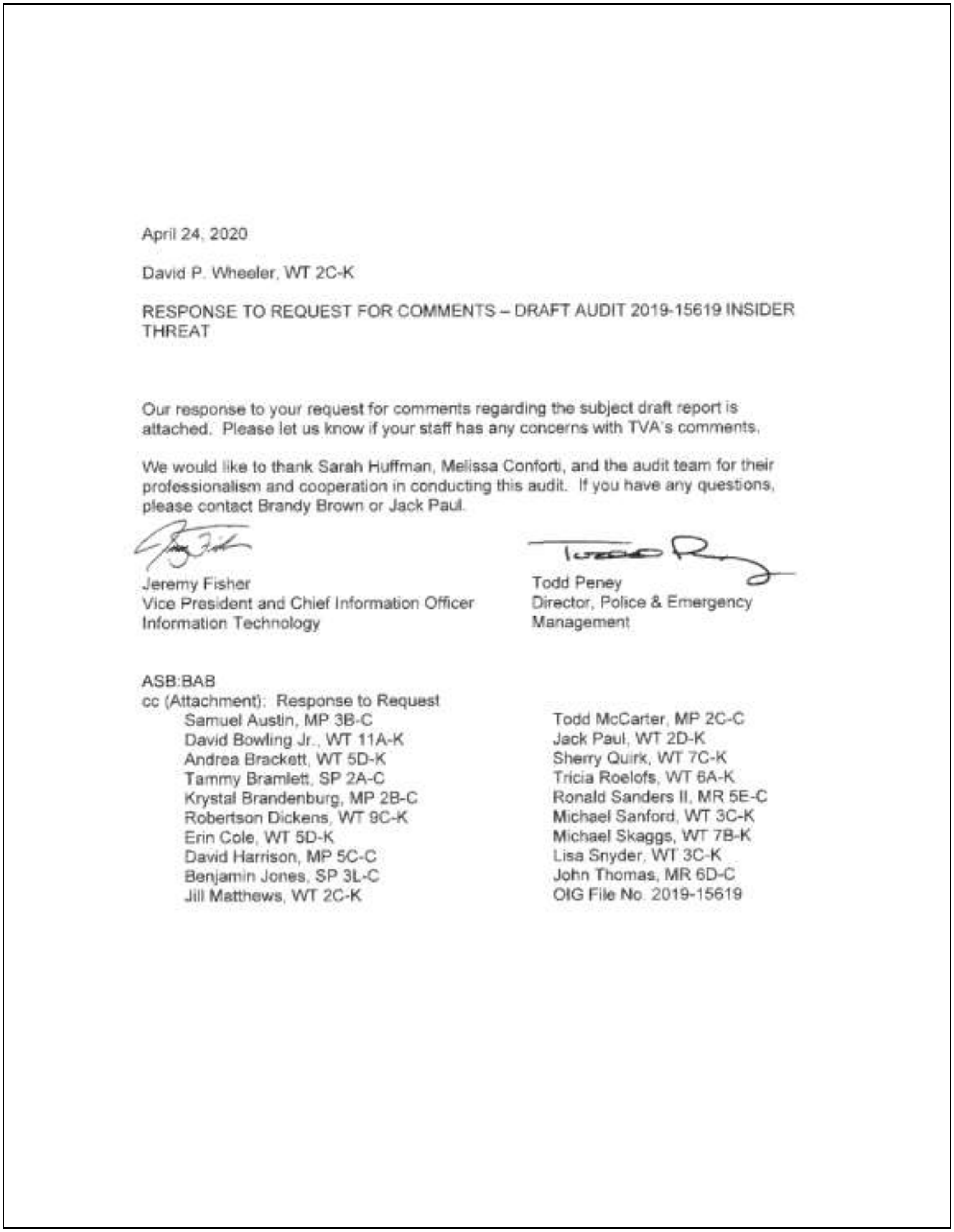
[5] "Department of Defense, Insider Threat Program – Best Practices – Hub Hiring," Rev. 2, May 24, 2017, <https://www.cdse.edu/documents/toolkits-insider/OUSDI-Personnel.pdf>, accessed on July 17, 2019.

The *2019 Insider Threat Program Maturity Model Report*[1] was created to help security professionals assess their organization‘s ability to monitor for, detect, and respond to insider threats. The definitions for the five levels of each maturity section are below:

Maturity Section	Nonexistent	Reactive	Proactive	Predictive	Optimized
Goals and Objectives	None	Respond to issues as they arise. Investigate as needed to identify what actions took place (if possible).	Monitor users with the highest risk to the organization for inappropriate activity.	Establish appropriate levels of monitoring to all Employees. Identify potential threats early. Respond appropriately to both leading and active indicators of threat activity.	Ensure the ITP meets the changing needs of the organization through review, adaptation, and optimization of processes, monitoring, and responses.
Awareness	The organization has zero visibility into employee activity, nor into whether they have been or are a victim of an insider threat.	The organization is generally aware of insider threats but are notified by employees or third-parties that an act has taken place.	The organization is aware of insider threats and is taking steps to monitor activity in an effort to detect malicious threats by users deemed high-risk to the organization.	The organization is highly aware of insider threats. While the focus is on malicious insiders, the organization is focused on identifying leading indicators of threats in an effort to stop threats before they occur.	The organization has a mature view of insider threat risk - seeing it as something that moves throughout the organization, with every employee as a potential threat. Every source of activity detail is used to provide a full picture of employee risk.
Governance	None	None	Minimally established governance. Informal interaction between Information Technology (IT), Human Resources (HR), and executive teams.	Oversight is established with a formalized team from IT, HR, executive, legal, and security. Threat definitions exist. Basic process and policies are in place.	ITP Team includes key employees and a designated senior ITP official to head the team. Written policies and processes exist. The ITP team meets using a regular cadence.
Risk Assessment	None	None	Identified high-risk individuals and roles requiring monitoring.	Risk levels are defined, high- and low-risk roles are assigned. Specific one-off risk assessments occur for individuals.	Risk reviews, reassignment of risk levels and associated monitoring actions occur regularly for both roles and individuals.
Policies	None	None	Either none, or basic policies exist for high-risk individuals, driven by HR or IT.	Policies exist around bring your own devices, proper use of company resources, and maintaining confidentiality.	Policies are routinely examined to ensure they align with other changes in the program.

[1] *2019 Insider Threat Program Maturity Model Report*, January 22, 2019, <https://www.prnewswire.com/news-releases/2019-insider-threat-program-maturity-model-report-released-300781612.html>, accessed on June 20, 2019.

Maturity Section	Nonexistent	Reactive	Proactive	Predictive	Optimized
Monitoring	None	None	Activity is monitored for pre-defined activity thresholds the organization equates as indicators of risk.	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.	Activity is monitored for both leading and active indicators of threats based on both static definitions and behavioral analysis.
Processes	None	None	Only informal processes exist around the review of activity and necessary response.	All employees are monitored for leading threat indicators using user behavior analytics and user activity monitoring. Clear and defined processes are in place for high-risk scenarios.	All employees are monitored for leading threat indicators utilizing user behavior analytics and user activity monitoring. Detailed processes are in place for specific low and high-risk scenarios, and are routinely evaluated and tested.
Intelligence Sources	None	None	Identified high-risk individuals and roles requiring monitoring.	Risk levels are defined, high- and low-risk roles are assigned. Specific one-off risk assessments occur for individuals.	Risk reviews, reassignment of risk levels and associated monitoring actions occur regularly for both roles and individuals.
Communications and Training	None	None	Basic acceptable use policy in place.	Acceptable use policy in used for all new hires.	Acceptable use policy & security acknowledgement are all signed by employees. Logon banners reaffirm proper usage, confidentiality, and security.



April 24, 2020

David P. Wheeler, WT 2C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2019-15619 INSIDER THREAT

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 Brandy Brown or Jack Paul.

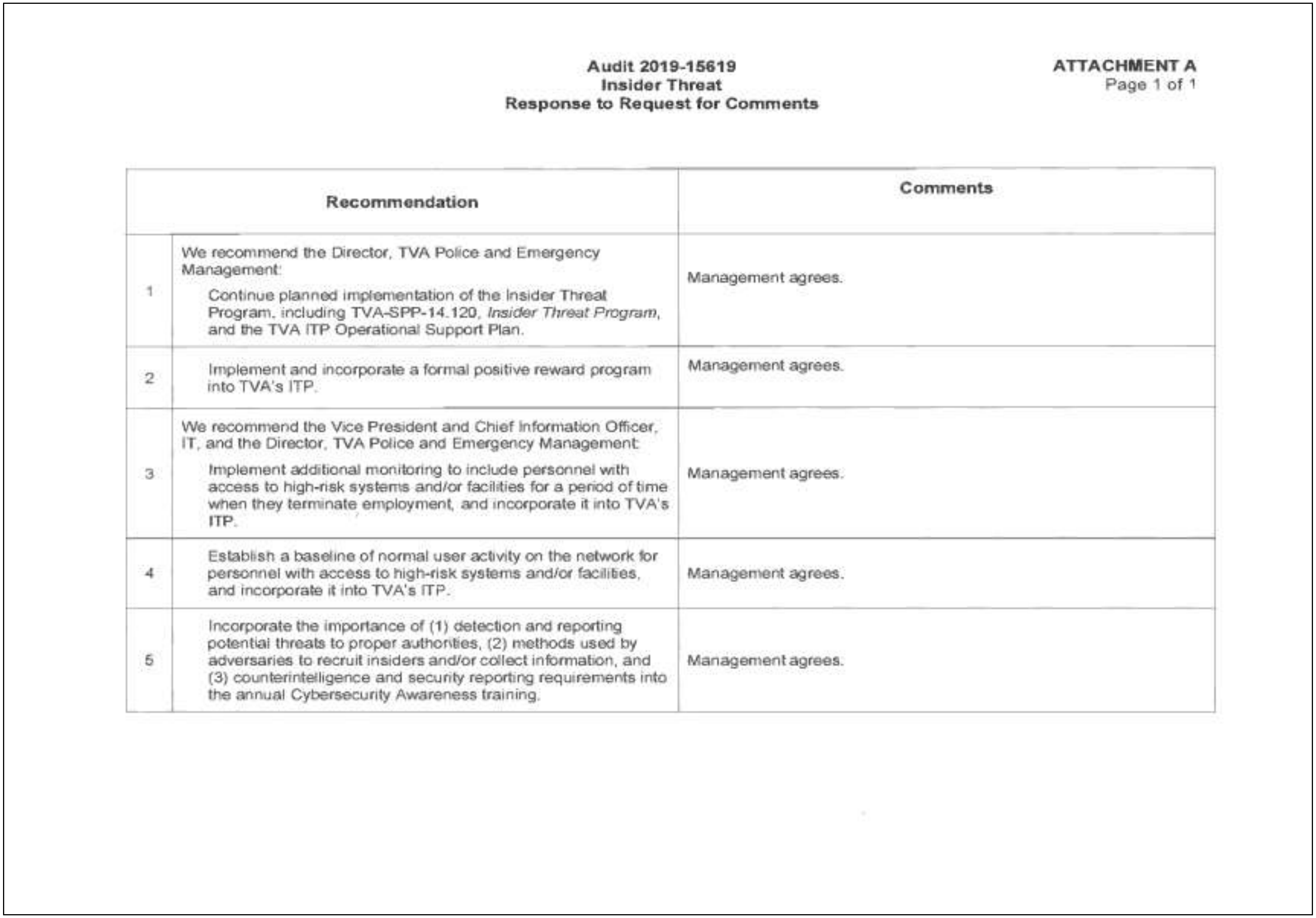
Jeremy Fisher
Vice President and Chief Information Officer
Information Technology

Todd Peney
Director, Police & Emergency
Management

ASB:BAB
cc (Attachment): Response to Request

Samuel Austin, MP 3B-C
David Bowling Jr., WT 11A-K
Andrea Brackett, WT 5D-K
Tammy Bramlett, SP 2A-C
Krystal Brandenburg, MP 2B-C
Robertson Dickens, WT 9C-K
Erin Cole, WT 5D-K
David Harrison, MP 5C-C
Benjamin Jones, SP 3L-C
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 II, 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. 2019-15619



ATTACHMENT A
Page 1 of 1

Audit 2019-15619
Insider Threat
Response to Request for Comments

Recommendation		Comments
1	We recommend the Director, TVA Police and Emergency Management: Continue planned implementation of the Insider Threat Program, including TVA-SPP-14.120, *Insider Threat Program*, and the TVA ITP Operational Support Plan.	Management agrees.
2	Implement and incorporate a formal positive reward program into TVA's ITP.	Management agrees.
3	We recommend the Vice President and Chief Information Officer, IT, and the Director, TVA Police and Emergency Management: Implement additional monitoring to include personnel with access to high-risk systems and/or facilities for a period of time when they terminate employment, and incorporate it into TVA's ITP.	Management agrees.
4	Establish a baseline of normal user activity on the network for personnel with access to high-risk systems and/or facilities, and incorporate it into TVA's ITP.	Management agrees.
5	Incorporate the importance of (1) detection and reporting potential threats to proper authorities, (2) methods used by adversaries to recruit insiders and/or collect information, and (3) counterintelligence and security reporting requirements into the annual Cybersecurity Awareness training.	Management agrees.