Memorandum from the Office of the Inspector General

July 27, 2016

John M. Hoskins, WT 9B-K

REQUEST FOR FINAL ACTION – AUDIT 2016-15377 – TVA'S FRAUD RISK MANAGEMENT

Fraud poses a significant risk to the integrity of federal programs and erodes public trust in government. Following the July 2015 issuance of the Government Accountability Office's (GAO) *A Framework for Managing Fraud Risks in Federal Programs* (Framework), we included an audit of the Tennessee Valley Authority's (TVA) fraud risk management activities on our annual audit plan. The objective of our audit was to determine if TVA had incorporated practices conducive to fraud risk management, as identified by GAO, in its organizational culture and structure.

In summary, we found while TVA has attempted to demonstrate a senior-level management commitment to integrity through various ethics and code of conduct policies, improvements are needed in TVA's practices to (1) combat fraud and (2) involve all levels of the agency in setting an antifraud tone. In addition, TVA management has not formally designated an entity to design and oversee fraud risk management activities.

We recommend TVA management consider (1) developing policies and practices that directly communicate the senior-level management commitment to combating fraud; (2) implementing practices, such as training and other fraud-awareness activities, that involve all levels of TVA in setting an antifraud tone that permeates the organizational culture; and (3) designating an entity within TVA to lead fraud risk management activities in accordance with the guidelines provided by the GAO Framework. TVA management agreed with our recommendations, stating they were consistent with Public Law 114-186 signed by President Obama on June 30, 2016. See Appendix B for TVA management's complete response.

BACKGROUND

The Association of Certified Fraud Examiners' (ACFE) 2016 *Report to the Nations on Occupational Fraud and Abuse* identifies three primary categories of occupational fraud: asset misappropriation, corruption, and financial statement fraud. According to the ACFE, asset misappropriation is by far the most common of the three primary categories of occupational fraud, consistently occurring in more than 83 percent of all cases reported to the ACFE with a median loss of $125,000. Approximately 35 percent of the cases the ACFE analyzed involved corruption with a median loss of $200,000. Financial statement

fraud was involved in less than 10 percent of the cases in the ACFE's study but had a median loss of $975,000.

In July 2015, the GAO's Framework was released to help managers combat fraud and preserve integrity in government agencies and programs. The Framework was also developed as a best practice to help agencies respond to the requirements of the revised *Standards for Internal Controls in the Federal Government* (Standards). The revised Standards became effective at the start of fiscal year 2016.

The Standards require managers to assess fraud risks as part of their internal control and would be considered a best practice for internal control in government. The GAO's Framework provides:

> Comprehensive guidance for conducting these assessments and using the results as part of the development of a robust antifraud strategy. It also describes leading practices for establishing an organizational structure and culture that are conducive to fraud risk management, designing and implementing controls to prevent and detect potential fraud, and monitoring and evaluating to provide assurance to managers that they are effectively preventing, detecting, and responding to potential fraud.

The Framework consists of four components for effectively managing fraud risks:

1. Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.

2. Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.

3. Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.

4. Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objective was to determine if TVA has incorporated practices conducive to fraud risk management, as identified by the GAO, in its organizational culture and structure. We restricted the scope of our audit to the implementation of the first component since the Framework was new to TVA. The first component of the Framework recommends that agencies commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management. Leading practices identified by GAO for creating a culture and structure to manage fraud risks include:

- Creating an organizational culture to combat fraud at all levels of the agency by:
  - Demonstrating a senior-level commitment to integrity and combating fraud, and
  - Involving all levels of the agency in setting an antifraud tone that permeates the organizational culture.

- Creating a structure with a dedicated entity to lead fraud risk management activities by designating an entity to design and oversee fraud risk management activities.

To achieve our audit objective, we:

- Interviewed TVA's (1) Sarbanes-Oxley (SOX) Director, (2) Chief Risk Officer, and (3) Enterprise Risk Management (ERM) Director.
- Reviewed TVA's current policies and documents addressing fraud controls and compared those activities to the leading practices outlined in the Framework. The documentation reviewed included the following:
  - TVA Code of Conduct
  - TVA Executive Code of Conduct
  - TVA Supplier Code of Conduct
  - TVA-Standard Programs and Processes (SPP)-11.8.1, Business Ethics
  - TVA-SPP-13.17, Enterprise Risk Management Policy
  - TVA-SPP-13.25, Sarbanes-Oxley Program
  - TVA Board of Director's Audit, Risk and Regulation Committee (ARRC) Charter
  - ARRC January 2015 meeting minutes
  - SOX Steering Committee April 21, 2015, meeting minutes
  - SOX fiscal year 2015 Fraud Risk Assessment
  - SOX 2016 antifraud controls
  - Enterprise Risk Council June 8, 2015, and December 7, 2015, meeting minutes

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.

FINDINGS

We found while TVA has attempted to demonstrate a senior-level management commitment to integrity through various ethics and code of conduct policies, improvements are needed in TVA's practices to (1) combat fraud and (2) involve all levels of the agency in setting an antifraud tone. In addition, TVA management has not formally designated an entity to design and oversee fraud risk management activities.

IMPROVEMENTS NEEDED IN TVA'S PRACTICES TO COMBAT FRAUD

We interviewed TVA personnel and reviewed policies and key SOX controls to determine if TVA had practices that create an organizational culture to combat fraud at all levels of the agency. We analyzed the information gathered from these interviews and documents to determine how they align with the practices outlined in the GAO's Framework. The Framework states that managers who effectively manage fraud risks (1) develop, document, and communicate an antifraud strategy that describes the agency's approach

to combating fraud; and (2) involve all levels of the agency in setting an antifraud tone that permeates the organizational culture. We determined that while TVA has attempted to demonstrate a senior-level management commitment to integrity through various ethics and code of conduct policies, improvements are needed in TVA's practices to (1) combat fraud and (2) involve all levels of the agency in setting an antifraud tone.

TVA currently assesses risk through the ERM program. According to TVA-SPP-13.17, Enterprise Risk Management Policy, the ERM approach used by TVA "endeavors to identify, analyze and evaluate enterprise risk in a systematic, comprehensive and effective manner." ERM utilizes inputs from multiple sources to develop a holistic and representative enterprise risk profile, which is continuously monitored based on internal and external developments. The ERM Policy also states, "Enterprise risk management is a collective effort of TVA employees and leadership." In addition to the ERM organization, TVA's enterprise risk structure also includes the:

- TVA Board-designated ARRC, whose primary purpose is to provide overall guidance;
- Enterprise Risk Council, whose primary purpose is to oversee TVA's management of enterprise risk; and
- Strategic Business Units, who are responsible for identifying risks and providing subject matter expertise to assess risks within their business units.

TVA's SOX Program Management Office (SOX PMO) classifies internal controls in three categories, one of which is entity-level controls. Entity-level controls focus on the broad goals of the organization and include controls around antifraud programs. In addition, as a part of TVA's adoption of the Committee of Sponsoring Organizations of the Treadway Commission's 2013 *Internal Control – Integrated Framework*, the SOX PMO completes fraud risk assessments. The risk assessment includes several business functions whose fraud awareness is deemed significant. According to TVA-SPP-13.25, Sarbanes-Oxley Program, the SOX PMO primarily uses its assessments to determine accounts and processes subject to testing and controls that should be documented to mitigate the risk of material misstatement in the financial statements.

In summary, while these practices address some fraud risks, improvements are needed to (1) combat fraud and (2) involve all levels of the agency in setting an antifraud tone. The GAO Framework's summary of the key elements of an antifraud strategy are included in Appendix A.

TVA MANAGEMENT HAS NOT FORMALLY DESIGNATED AN ENTITY TO DESIGN AND OVERSEE FRAUD RISK MANAGEMENT ACTIVITIES

We interviewed TVA personnel to determine if a structure with a dedicated entity to lead fraud risk management activities was present. TVA personnel informed us no entity had been formally designated to lead fraud risk management activities. In addition, TVA personnel informed us they view the Office of the Inspector General (OIG) as one of the primary managers of fraud risk. While our mission includes preventing and detecting fraud, waste, and abuse at TVA, responsibility for managing overall fraud risk resides with TVA management. The Framework states that the dedicated entity should be located

within the agency and not the OIG, so the latter can retain its independence to serve its oversight role.

The Framework also identified leading practices related to the antifraud entity's responsibilities. Specifically, the entity:

- Serves as the repository of knowledge on fraud risks and controls,
- Manages the fraud risk management process, and
- Leads or assists with training and other fraud-awareness activities.

TVA personnel informed us various groups within TVA share responsibilities to manage risk. We analyzed documentation related to the fraud risk management responsibilities for each of these groups and determined the following:

- **ERM Organization** – According to the ERM Policy, TVA's ERM organization is responsible for promoting a culture of effective risk management, developing risk management methodologies and tools, conducting and supporting risk identification and analysis activities, developing an overall TVA risk profile, and reporting the key enterprise risks to the Enterprise Risk Council and the TVA Board's ARRC. Based on our analysis of the ERM Policy and the roles of each of these groups, we noted this responsibility does not specifically address fraud risk management.
- **SOX PMO** – The SOX PMO performs periodic fraud inquiries and assessments as a part of its scoping activities. We determined these assessments are primarily used to determine accounts and processes subject to testing and controls that should be documented to mitigate the risk of material misstatements in the financial statements. The SOX PMO does not address risks associated with asset misappropriation or corruption.
- **TVA Ethics Program** – According to TVA's Ethics Web site, the "ethics program helps employees support the integrity and efficiency of TVA operations, make the right decisions for the right reasons, and maintain public confidence." We noted TVA-SPP-11.8.1, Business Ethics, does not directly address fraud risk management.

In summary, we determined these groups do not function as entities that oversee fraud risk management as defined by the GAO Framework.

RECOMMENDATIONS

We recommend TVA management consider:

1. Developing policies and practices that directly communicate the senior-level management commitment to combating fraud.

2. Implementing practices, such as training and other fraud-awareness activities, that involve all levels of TVA in setting an antifraud tone that permeates the organizational culture.

3. Designating an entity within TVA to lead fraud risk management activities in accordance with the guidelines provided by the GAO Framework.

TVA Management's Comments – TVA management agreed with our recommendations, stating they were consistent with Public Law 114-186 signed by President Obama on June 30, 2016. TVA management stated ERM will work with executives and appropriate business units to develop policies and practices that directly communicate the senior-level commitment to combating fraud. In addition, ERM will work with the Office of the General Counsel to implement fraud awareness training as part of TVA's required annual training. On August 10, 2016, TVA will meet with the ARRC and recommend formal designation of ERM as the organization to design and oversee fraud risk management activities. ERM will update the OIG on the progress in these areas during the next year. See Appendix B for TVA management's complete response.

- - - - - -

This report is for your review and final action. Your written comments, which addressed your management decision and actions planned or taken, have been included in the report. Please notify us when final action is complete. In accordance with the Inspector General Act of 1978, as amended, the OIG is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

Information contained in this report may be subject to public disclosure. Please advise us of any sensitive information in this report that you recommend be withheld.

If you have any questions or need additional information, please contact Chasity W. Scantling, Auditor, at (865) 633-7358 or Rick C. Underwood, Director, Financial and Operational Audits, at (423) 785-4284. 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)
ET 3C-K

CWS:BSC
Attachment
cc (Attachment):

TVA Board of Directors
Robertson D. Dickens, WT 4D-K
J. David Gamble, WT 4D-K
William D. Johnson, WT 7B-K
R. Heath Jones, WT 9B-K
Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Richard W. Moore, ET 4C-K
John M. Thomas III, MR 6D-C
Tammy W. Wilson, WT 4C-K
OIG File No. 2016-15377

KEY ELEMENTS OF AN ANTIFRAUD STRATEGY[1]

Table 4: Key Elements of an Antifraud Strategy	
Who is responsible for fraud risk management activities?	Establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General (OIG) to investigate potential fraud.
What is the program doing to manage fraud risks?	Describe the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.[a]
When is the program implementing fraud risk management activities?	Create timelines for implementing fraud risk management activities, as appropriate, including monitoring and evaluations.
Where is the program focusing its fraud risk management activities?	Demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile.
Why is fraud risk management important?	Communicate the antifraud strategy to employees and other stakeholders, and link antifraud efforts to other risk management activities, if any.

[1] *A Framework for Managing Fraud Risks in Federal Programs*, United States Government Accountability Office, July 2015, p. 19.

July 21, 2016

David P. Wheeler, ET 3C-K

COMMENTS - DRAFT AUDIT 2016-15377 - TVA'S FRAUD RISK MANAGEMENT

We appreciate the recommendations from the OIG to improve TVA's fraud risk management practices. Based on our review and understanding, these recommendations are consistent with Public Law No. 114-186 signed by President Obama on June 30, 2016.

Therefore at the Audit, Risk, and Regulation Committee meeting on August 10th, TVA will recommend and formally designate that Enterprise Risk Management (ERM) be the organization to design and oversee fraud risk management activities. ERM will work with executives and appropriate business units to develop policies and practices that directly communicate the senior-level management commitment to combating fraud. ERM will also work with the Office of the General Counsel (OGC) to implement fraud awareness training as part of TVA's required annual trainings.

ERM will report on the progress in these areas to the OIG during the next year. We appreciate the professional manner utilized by the OIG staff throughout this review.

Tammy W. Wilson
Vice-President, Treasurer & Chief Risk Officer
Financial Services
WT 4C-K

cc: John M. Thomas III, MR 6D-C
Robertson D. Dickens, WT 4D-K
J. David Gamble, WT 4D-K
John M. Hoskins, WT 9A-K
R. Heath Jones, WT 9B-K
Dwain K. Lanier, MR 6D-C
Diane T. Wear, WT 4 4B-K

OIG File No. 2016-15377