Memorandum from the Office of the Inspector General

April 16, 2019

Jeremy P. Fisher, SP 3A-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2018-15598 – INFORMATION SYSTEMS CATEGORIZATION PROCESS

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 Jonathan B. Anderson, Senior Auditor, at (865) 633-7340 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)
WT 2C-K

JBA:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Clifford L. Beach Jr., WT 7B-K
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
Dwain K. Lanier, MR 6D-C
Jeffery J. Lyash, WT 7B-K
Justin C. Maierhofer, WT 7B-K
Jill M. Matthews, WT 2C-K
Todd E. McCarter, MP 2C-C
Sherry A. Quirk, WT 7C-K
John M. Thomas III, MR 6D-C
Rebecca C. Tolene, WT 7B-K
OIG File No. 2018-15598

TVA RESTRICTED INFORMATION

Office of the Inspector General

Audit Report

To the Vice President and
Chief Information Officer,
Information Technology

INFORMATION SYSTEMS CATEGORIZATION PROCESS

Audit Team
Jonathan B. Anderson
Frank B. Lord II

Audit 2018-15598
April 16, 2019

ABBREVIATIONS

FIPS	Federal Information Processing Standards
ISO	Information System Owner
NIST	National Institute of Standards and Technology
SP	Special Publication
SPP	Standard Programs and Processes
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

APPENDICES

Audit 2018-15598 – Information Systems Categorization Process

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Federal Information Security Management Act of 2002 tasked the National Institute of Standards and Technology (NIST) with development responsibilities for categorizing information systems including:

- Standards to be used by all federal agencies to categorize all information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate level of information security according to a range of risk levels; and
- Guidelines recommending the types of information and information systems to be included in each category.

Tennessee Valley Authority (TVA) Cybersecurity has an information systems categorization process in place where the information system owner and steward(s) assess the potential impact that a loss of confidentiality, integrity, or availability of an information system would have on TVA. This is to help prevent events from occurring that would jeopardize TVA's ability to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, or protect individuals. The resulting system's federal information processing standards (FIPS) categorization from the process influences the security controls selected for securing the system.

We scheduled this audit due to the risk of information systems being incorrectly categorized, which could result in systems not receiving the appropriate tools, resources, or security. Our objective was to determine if TVA's information systems categorization process was effective and in compliance with FIPS Publication 199 and NIST Special Publication (SP) 800-60. Our audit scope was information systems subject to the categorization process performed by TVA Cybersecurity.

What the OIG Found

We determined that portions of TVA's information systems categorization process were effective. Specifically, we found TVA's process was (1) designed in alignment with the agency's mission and FIPS Publication 199, (2) well understood by TVA Cybersecurity personnel, and (3) clearly documented. However, we found gaps with implementing NIST SP 800-60 guidance. Specifically, we found (1) we could not verify that TVA considered NIST system factors in the systems categorization process, (2) consideration and documentation for interconnecting systems was inconsistent, (3) not all categorized systems were revisited every three years, and (4) several Web sites, systems and/or subcomponents for larger systems were not categorized.

What the OIG Recommends

We recommend the Vice President and Chief Information Officer, Information Technology, take the following actions:

1. Improve documentation to support both information and system considerations from NIST guidance when determining the system's overall categorization, or FIPS rating.

2. Ensure interconnecting systems are identified and documented consistently and considered appropriately in the categorization process.

3. Update the categorization process to require systems be revisited in accordance with NIST guidance.

4. Develop plans to ensure all applicable systems (i.e., Web sites, privacy related systems, supporting systems, and/or subcomponents) go through the information systems categorization process and are recorded appropriately in the asset management tool.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with the audit findings and recommendations. See Appendix B for TVA management's complete response.

BACKGROUND

The Federal Information Security Management Act of 2002 tasked the National Institute of Standards and Technology (NIST) with development responsibilities for categorizing information systems including:

- Standards to be used by all federal agencies to categorize all information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate level of information security according to a range of risk levels; and
- Guidelines recommending the types of information and information systems to be included in each category.

Federal Information Processing Standards (FIPS) Publication 199[1] addresses the first task by developing standards for categorizing information and information systems.[2] NIST Special Publication (SP) 800-60[3] addresses the second task by developing guidelines recommending the types of information and information systems to be included in each category.

Tennessee Valley Authority (TVA) Cybersecurity has an information systems categorization process in place where the information system owner (ISO) and steward(s) assess the potential impact that a loss of confidentiality, integrity, or availability of an information system would have on TVA. This is to help prevent events from occurring that would jeopardize TVA's ability to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, or protect individuals. The resulting system's FIPS categorization from the process influences the security controls selected for securing the system. TVA categorizations are shown in Table 1.

Categorization	Potential Impact
High	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Table 1

[1] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[2] Information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations.

[3] NIST SP 800-60 Volume I Revision 1, *Guide for Mapping Types of Information Systems to Security Categories*, August 2008.

We scheduled this audit due to the risk of information systems being incorrectly categorized, which could result in systems not receiving the appropriate tools, resources, or security.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if TVA's information systems categorization process is effective and in compliance with FIPS Publication 199 and NIST SP 800-60. Our audit scope was information systems subject to the categorization process performed by TVA Cybersecurity. Our fieldwork was performed between October 2018 and January 2019. A complete discussion of our audit objective, scope, and methodology is included in Appendix A.

FINDINGS

In summary, we determined that portions of TVA's information systems categorization process were effective. Specifically, we found TVA's process was (1) designed in alignment with the agency's mission and FIPS Publication 199, (2) well understood by TVA Cybersecurity personnel, and (3) clearly documented. However, we found gaps with implementing NIST SP 800-60 guidance. Specifically, we found (1) we could not verify that TVA considered NIST system factors in the systems categorization process, (2) consideration and documentation for interconnecting systems was inconsistent, (3) not all categorized systems were revisited every three years, and (4) several Web sites, systems and/or subcomponents for larger systems were not categorized.

GAPS WITH IMPLEMENTING NIST GUIDANCE

NIST SP 800-60 includes a number of system factors that should be considered during information systems categorization. The system factors include (1) aggregation, (2) critical system functionality, (3) extenuating circumstances, (4) public information integrity [or Web sites/Web pages], (5) catastrophic loss of system availability, (6) large supporting and interconnecting systems, (7) critical infrastructures and key resources, (8) privacy information, and (9) trade secrets. TVA personnel informed us these factors are considered during the systems categorization process. However, we found that except for some interconnecting systems, TVA's information systems categorization process did not document consideration of these NIST system factors. Accordingly, we could not verify whether these factors were considered in the categorization process. We also found documentation for interconnecting systems was inconsistent.

Unable to Verify NIST System Factors Were Considered

We found that TVA's information systems categorization process did not document consideration of the NIST system factors specific to aggregation, critical system functionality, extenuating circumstances, catastrophic loss of system availability, and some interconnecting systems. Accordingly, we could not verify whether these factors were considered in the categorization process.

TVA Cybersecurity holds a meeting involving the following stakeholders who are ultimately responsible for determining the system categorization for each system subject to the information systems categorization process:

- ISO
- Information steward(s)
- Cybersecurity liaison

These meetings determine the information types within the system and NIST system factors that may also impact the categorization. We interviewed several stakeholders and observed one meeting. We found these meetings produced a document signed by the ISO showing the information types pertinent to the system, along with the objective and impact level for each information type that results in an overall system categorization, or FIPS rating.

TVA currently has five systems categorized as “High”. According to TVA, the current categorization process is more focused on data availability protection than system availability. The risk of incorrect system categorization increases if system categorization is based solely on information types and system factors are not also appropriately considered.

Inconsistencies in Considering and Documenting Interconnecting Systems
NIST guidance states that a system’s interconnecting systems[4] are to be considered in determining categorization. We reviewed the interconnecting systems for the critical infrastructure related systems that support TVA’s mission. We found four systems appropriately considered and documented their interconnecting systems. However, we also found documentation for:

- Three systems mentioned having interconnections but did not identify actual interconnecting systems.
- Two systems identified multiple interconnecting systems, but not all of the interconnecting systems had been evaluated for categorization, or had FIPS ratings.

In addition, interconnecting systems for one system could not be confirmed.

The categorization of an interconnected system may influence the categorization of the system being categorized. Therefore, inconsistent documentation of interconnecting systems increases the risk of incorrect system categorizations.

[4] For purposes of this audit, we defined interconnecting systems as any system that transfers data into another system via automated jobs or acts as a bridge between two or more other systems.

SYSTEM CATEGORIZATIONS SHOULD BE REVISITED AT LEAST EVERY THREE YEARS

NIST SP 800-60 guidance states that system categorizations should be revisited at least every three years or when a significant change occurs to the system or supporting business lines. We reviewed information systems categorization process documents, including TVA standard programs and processes (SPP) and completed information system categorizations, to determine if categorized systems were being revisited within three years.

We found the three year cadence was not included in TVA policy. Specifically, TVA-SPP-12.800, *Risk Management Framework,* communicated information system categorizations should be reviewed as systems progress through the system development life cycle, especially when significant changes occur. However, the SPP does not require categorization to be revisited at least every three years.

We reviewed 37 information systems categorization documents dated from June 17, 2015, to October 17, 2018. We found 32 were revisited for categorization within three years. However, we could not confirm that the remaining 5 systems had been revisited due to a lack of documentation. According to TVA Cybersecurity personnel:

- Three of the five systems were not revisited within three years for categorization because they were considered low risk. Since these systems were already categorized as “Low”, TVA Cybersecurity determined to review these at a future date after they have evaluated systems categorized “High”, “Moderate”, or that have never been evaluated.
- One information system categorization was revisited, but no date was recorded documenting when it was revisited.
- One information system was revisited and determined to no longer be in use and was to be retired. However, TVA management did not provide documentation to support this.

SYSTEMS NOT CATEGORIZED

TVA has an asset management tool that records the categorization for all systems subject to the categorization process. The asset management tool also (1) tracks which systems have not been evaluated for categorization, and (2) identifies which systems are Web sites; privacy information related systems; and/or subcomponents for larger systems. We reviewed TVA’s system inventory and found the following were not categorized:

- Seventy-five Web sites.
- Nineteen privacy information related systems.

- Forty-six subcomponents for larger systems.

These Web sites, systems, and system subcomponents are subject to the information systems categorization process but had not been evaluated. According to TVA personnel, these have not been evaluated due to the backlog of systems requiring evaluation.

RECOMMENDATIONS

We recommend the Vice President and Chief Information Officer, Information Technology:

1. Improve documentation to support both information and system considerations from NIST guidance when determining the system's overall categorization, or FIPS rating.

2. Ensure interconnecting systems are identified and documented consistently and considered appropriately in the categorization process.

3. Update the categorization process to require systems be revisited in accordance with NIST guidance.

4. Develop plans to ensure all applicable systems (i.e., Web sites, privacy related systems, supporting systems, and/or subcomponents) go through the information systems categorization process and are recorded appropriately in the asset management tool.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with the audit findings and recommendations. See Appendix B for TVA management's complete response.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if the Tennessee Valley Authority's (TVA) information systems categorization process is effective and in compliance with the Federal Information Processing Standards (FIPS) Publication 199[1] and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60.[2] Our audit scope was information systems subject to the categorization process performed by TVA Cybersecurity. Fieldwork was performed between October 2018 and January 2019.

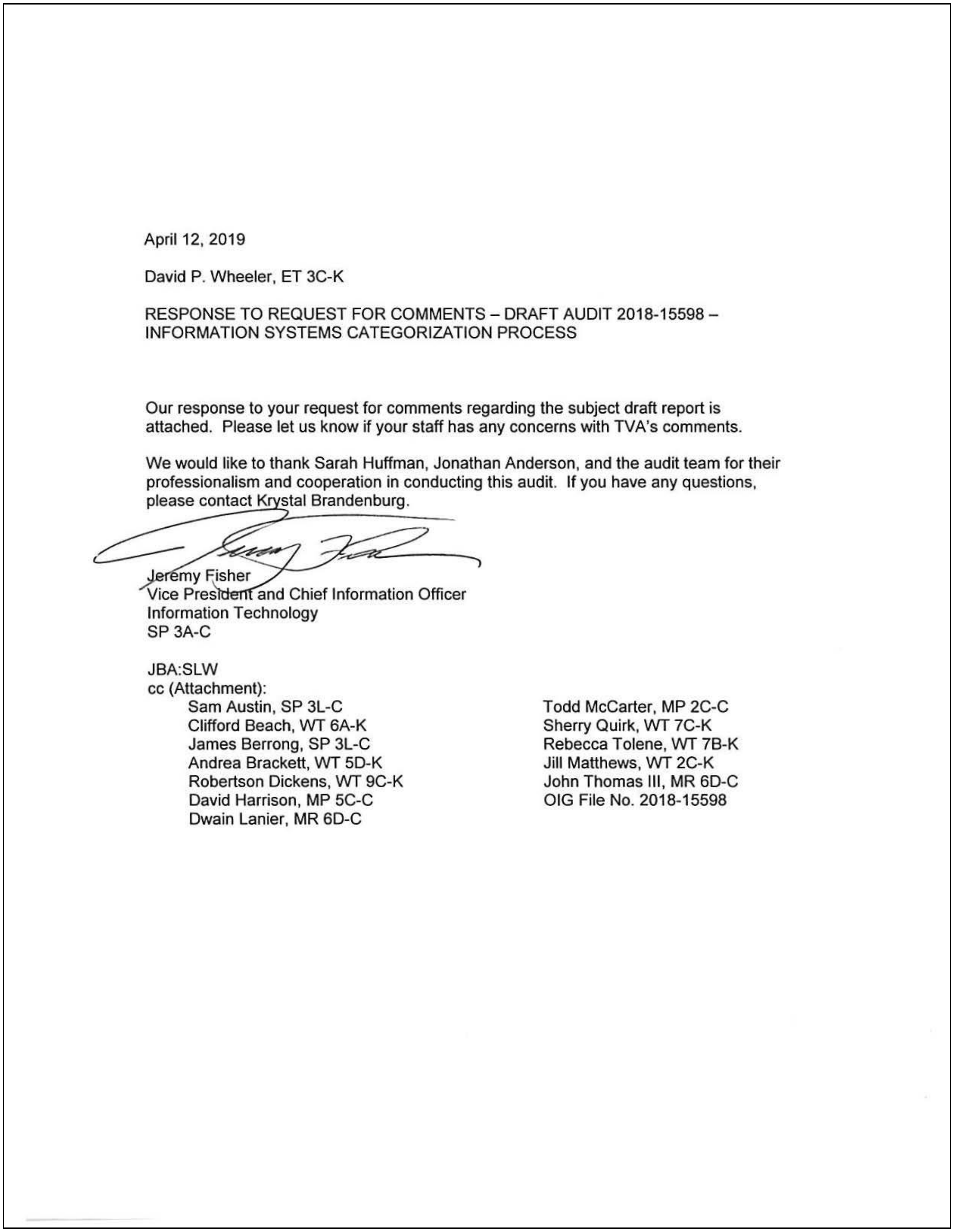
To achieve our objective, we:

- Identified and interviewed stakeholders within the process to understand how categorization was determined.
- Reviewed applicable TVA Standard Programs and Processes (SPP) to obtain an understanding of the categorization process, including:
  - TVA-SPP-12.002, *TVA Information Management Policy*
  - TVA-SPP-12.011, *Service Level Management*
  - TVA-SPP-12.800, *Risk Management Framework*
- Obtained and reviewed FIPS Publication 199 and NIST SP 800-60 guidance to determine criteria specific to our audit objective.
- Identified information types used by TVA and performed a gap analysis using TVA's mission statement and organization charts as of September 7, 2018, to ensure alignment with the mission.
- Interviewed TVA Cybersecurity personnel to understand how each NIST factor is taken into consideration at TVA.
- Reviewed TVA's asset management system for systems subject to the categorization process to determine systems that have been / have not been through the categorization process.
- Reviewed system security plans and FIPS Publication 199 workbooks for critical infrastructure related systems to determine supporting and interconnecting systems.
- Reviewed categorization documentation for the 37 information systems identified by TVA Cybersecurity to determine if any of the categorized systems were revisited within three years.
- Attended a FIPS meeting on January 15, 2019, to note attendance and observe how FIPS and NIST guidance were applied.

[1] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004.

[2] NIST Special Publication 800-60 Volume I Revision 1, *Guide for Mapping Types of Information Systems to Security Categories*, August 2008.

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.



April 12, 2019

David P. Wheeler, ET 3C-K

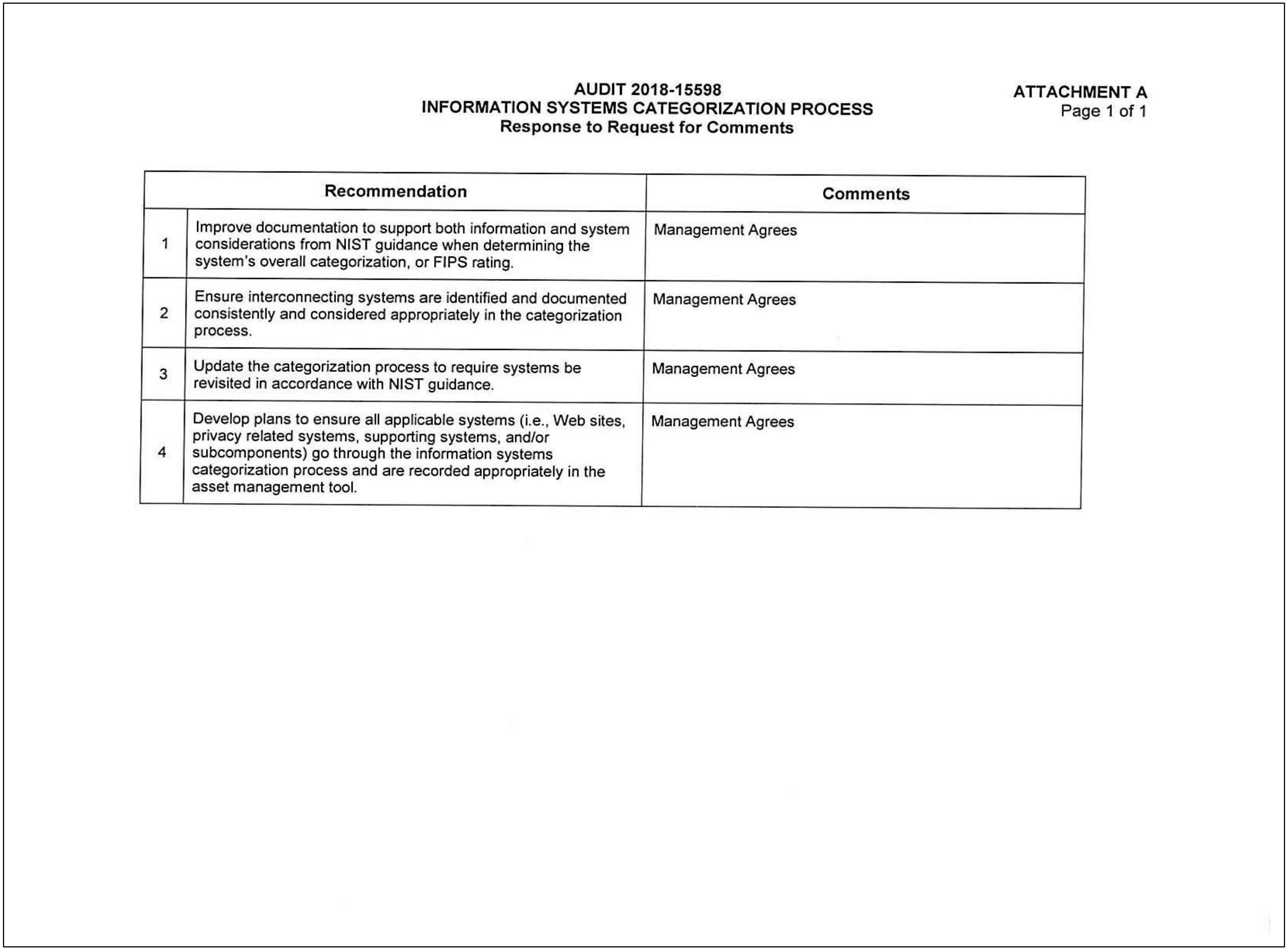
RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2018-15598 –
INFORMATION SYSTEMS CATEGORIZATION PROCESS

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, Jonathan Anderson, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg.

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

JBA:SLW
cc (Attachment):
Sam Austin, SP 3L-C
Clifford Beach, WT 6A-K
James Berrong, SP 3L-C
Andrea Brackett, WT 5D-K
Robertson Dickens, WT 9C-K
David Harrison, MP 5C-C
Dwain Lanier, MR 6D-C
Todd McCarter, MP 2C-C
Sherry Quirk, WT 7C-K
Rebecca Tolene, WT 7B-K
Jill Matthews, WT 2C-K
John Thomas III, MR 6D-C
OIG File No. 2018-15598



ATTACHMENT A
Page 1 of 1

AUDIT 2018-15598
INFORMATION SYSTEMS CATEGORIZATION PROCESS
Response to Request for Comments

Recommendation		Comments
1	Improve documentation to support both information and system considerations from NIST guidance when determining the system's overall categorization, or FIPS rating.	Management Agrees
2	Ensure interconnecting systems are identified and documented consistently and considered appropriately in the categorization process.	Management Agrees
3	Update the categorization process to require systems be revisited in accordance with NIST guidance.	Management Agrees
4	Develop plans to ensure all applicable systems (i.e., Web sites, privacy related systems, supporting systems, and/or subcomponents) go through the information systems categorization process and are recorded appropriately in the asset management tool.	Management Agrees