Memorandum from the Office of the Inspector General

August 28, 2017

David W. Sorrick, LP 3K-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2017-15452 – GAS SECURE ROOM CYBER SECURITY

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.

If you have any questions or wish to discuss our findings, please contact Michael P. Anderson, Senior Auditor, at (865) 633-7393 or Scott A. Marler, Director (Acting), Information Technology Audits, at (865) 633-7352. 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

MPA:BSC
Attachment
cc (Attachment):
TVA Board of Directors
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Josh T. Brewer, LP 2G-C
Robertson D. Dickens, WT 9C-K
Joe P. Grimes, LP 6A-C
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Richard W. Moore, ET 4C-K
David P. Moran, LP 2G-C
Stacey L. Parrott, LP 2G-C
Philip D. Propes, MP 2C-C
Scott D. Self, SP 3A-C
OIG File No. 2017-15452

Office of the Inspector General

Audit Report

To the Senior Vice President, Power Operations

GAS SECURE ROOM CYBER SECURITY

Audit Team
Michael P. Anderson
Jessie A. Bradford
Scott A. Marler
Megan E. Spitzer

Audit 2017-15452
August 28, 2017

SYNOPSIS

The Office of the Inspector General performed an audit of cyber security at two gas secure rooms that provide remote logical access to all TVA gas-fired plants. Our objective was to determine if the gas secure rooms have appropriate logical and physical security controls in place to ensure authorized access to the Tennessee Valley Authority's (TVA) combustion turbine (CT) and combined cycle (CC) control networks.

In summary, we found the architecture, current standard programs and processes, and draft standard operating procedures contain appropriate information as suggested by best practices. However, we found the logical controls for the gas secure rooms could be strengthened. Specifically, we found issues with the (1) network devices at the gas secure rooms and a sample of CC and CT plants and (2) workstations and servers at the gas secure rooms. Additionally, we found the gas secure rooms were not being used for access as originally intended.[1]

We made seven specific recommendations to management to help strengthen the logical controls related to the gas secure rooms, including reevaluating the need for the physical gas secure rooms. Our specific recommendations are included at the end of this report.

TVA Management's Comments – TVA management agreed with our findings and recommendations and requested additional verbiage in (1) the Synopsis about an ongoing project to enhance the security of remote access from the gas secure rooms and (2) specific recommendations. See the Appendix for TVA management's complete response.

Auditor's Response – We reviewed TVA management's comments and added verbiage to the Background section to include information on the ongoing project to implement the gas secure rooms. However, the recommendation verbiage was not added as TVA management has the option to accept and document risk in their management action plan.

BACKGROUND

TVA's gas-fired power plants provided 10,310 megawatts of net summer generation capability (approximately 31.5 percent of net TVA-operated summer generation capability) as of September 30, 2016. Without proper logical and physical access controls, these resources could be accessed by unauthorized individuals, thereby allowing access to gas plants that could lead to interruption of power production at that facility.

[1] Specifics of the identified issues have been omitted from this report due to their sensitive nature but were formally communicated to TVA management in a debriefing on June 15, 2017.

During our audit of cyber security at a power generation facility,[2] we learned of the existence of two gas secure rooms that provide remote logical access to all TVA gas-fired plants. Power Operations launched a project in 2014 to establish the gas secure rooms that included updating the architecture for remote access. While this project was still ongoing during our audit, remote access for TVA employees had been established and was in use. Due to the nature of this access, we scheduled an audit of the gas secure rooms to determine if appropriate logical and physical security controls are in place.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if the gas secure rooms have appropriate logical and physical security controls in place to ensure authorized access to TVA's CT and CC control networks. Our scope included the two gas secure rooms and their network connections to the gas plants. To achieve our objective, we:

- Reviewed documentation and interviewed TVA's Generation Cyber Security personnel to obtain an understanding of the gas secure rooms.
- Performed a gap analysis of current and draft TVA policies and procedures governing the gas secure room against best practices.
- Reviewed the architecture of the gas secure rooms setup against best practices.
- Visited the gas secure rooms to review physical security controls in place.
- Visited a sample of three of six TVA CC plants and one of nine TVA CT plants to review physical security controls in place at network closets/cabinets that provide network connectivity to the gas secure rooms. We judgmentally selected the sample based on TVA's risk ranking of plants, megawatt output of the plants, and gas turbine vendor uniqueness. We selected one CT plant based on its location adjacent to a CC plant in our sample. Since this was a judgmental sample, the results of the sample cannot be projected to the population.
- Obtained and reviewed configurations from the full population of network devices at the gas secure rooms and firewalls from the CT and CC plants and compared those configurations against TVA baselines and best practices.
- Obtained and reviewed configurations from the full population of servers and desktops at the gas secure rooms and compared those configurations against best practices.

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.

[2] Audit Report 2015-15286, Power Generation Facility Cyber Security, April 20, 2016.

FINDINGS

We found the architecture, current standard programs and processes, and draft standard operating procedures contain appropriate information as suggested by best practices. However, we found the logical controls for the gas secure rooms could be strengthened. Specifically, we found issues with the (1) network devices at the gas secure rooms and a sample of CC and CT plants and (2) workstations and servers at the gas secure rooms. Additionally, we found the gas secure rooms were not being used for access as originally intended. (Specifics of the identified issues have been omitted from this report due to their sensitive nature but were formally communicated to TVA management in a debriefing on June 15, 2017.)

NETWORK DEVICE ISSUES

We reviewed the network devices at the gas secure rooms as well as a sample of CC and CT plants. We reviewed the configurations of those devices against the standard TVA baseline of configuration settings and found all 12 devices we reviewed did not fully meet the TVA baseline. Standard baselines are designed to help validate security of devices. Devices that do not meet baselines are at an increased risk of compromise due to configurations not being as expected.

In addition, we found 1 firewall that was running an unsupported operating system. Devices running unsupported operating systems do not receive security patches or reliability updates, which puts them at an increased risk of compromise as unpatched systems allow exploitation of flaws to gain unauthorized access.

WORKSTATION AND SERVER ISSUES

We reviewed the configurations of six workstations and nine servers (collectively referred to as computer devices) in the gas secure rooms against best practices. In summary, we found:

- Two of the computer devices were running unsupported life operating systems. Computer devices running unsupported operating systems do not receive security patches, which increases the risk of compromise.
- All 15 of the computer devices had out-of-date security patches. Computer devices with out-of-date security patches increase the risk of compromise as unpatched systems allow exploitation of flaws to gain unauthorized access.
- Five of the computer devices had unneeded accounts on them. Unneeded accounts give attackers another method to compromise systems.

Additionally, we found baseline configurations have not been implemented for the servers and workstations in the gas secure rooms managed by Generation Engineering. Baseline configurations help ensure standard settings are applied to devices.

GAS SECURE ROOMS NOT BEING USED FOR ACCESS AS ORIGINALLY INTENDED

The gas secure rooms were originally intended to be a secure room where TVA engineers could log into a workstation and access the gas plants via a secure remote access connection. The engineers now have the capability to access gas plants via the secure remote access connection from outside a gas secure room and do not have to physically be in the gas secure room. Additionally, TVA personnel informed us TVA plans to move the network and server infrastructure that enables this secure remote access from the gas secure rooms to a TVA Information Technology data center. As a result, the gas secure rooms may no longer be needed.

RECOMMENDATIONS

We recommend the Senior Vice President, Power Operations:

1. Ensure all network devices in the gas secure rooms and at the CC and CT plants meet standard TVA baselines and document any deviations from those baselines.
2. Ensure all network devices in the gas secure rooms and at CC and CT plants run currently supported operating systems.
3. Ensure all servers and workstations in the gas secure rooms run supported operating systems.
4. Ensure all servers and workstations in the gas secure rooms are appropriately patched.
5. Remove unneeded accounts from the servers and workstations in the gas secure rooms.
6. Define and implement baseline configurations for the servers and workstations in the gas secure rooms.
7. Reevaluate the continued need for the physical gas secure rooms.

TVA Management's Comments – TVA management agreed with our findings and recommendations and requested additional verbiage in (1) the Synopsis about an ongoing project to enhance the security of remote access from the gas secure rooms and (2) specific recommendations. See the Appendix for TVA management's complete response.

Auditor's Response – We reviewed TVA management's comments and added verbiage to the Background section to include information on the ongoing project to implement the gas secure rooms. However, the recommendation verbiage was not added as TVA management has the option to accept and document risk in their management action plan.

August 16, 2017

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2017-15452 – GAS SECURE ROOM CYBER SECURITY

Our response to your request for comments regarding the findings of 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 Michael Anderson, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Tommy Johnson at 256-386-2822, or Josh Brewer at 423-751-2456.

David W. Sorrick

David W. Sorrick
Sr. Vice President
Power Operations
LP 3K-C

cc (Attachment):

Andrea S. Brackett, WT 5D-K
Krystal R. Brandenburg, MP 3C-C
Patrick Y. Buchanan, WT 5D-K
Clay DeLoach, Jr., SP 3L-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MR 6D-C
Dwain K. Lanier, MR 6D-C
Richard W. Moore, ET 4C-K
Philip D. Propes, MP 3B-C
John M. Thomas III, MR 6D-C
Stacey L. Parrott, LP 2G-C
David P. Moran, LP 2G-C
Josh T. Brewer, LP 2G-C
OIG File No. 2017-15452

AUDIT 2017-15452
Gas Secure Room Cyber Security
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

Page	Draft Report Section	Comments
1	Synopsis	Management respectfully requests considering adding to beginning of paragraph two: "This audit was conducted while an active project to enhance the security of remote access managed from the gas secure rooms was "in progress". Recommendations can be incorporated into the project scope to ensure cyber security controls for remote access is strengthened before project closure."

	Recommendation	Risk	Management Comments
1	Ensure all network devices in the gas secure rooms and at the CC and CT plants meet standard TVA baselines and document any deviations from those baselines.	Low	Management agrees.
2	Ensure all network devices in the gas secure rooms and at the CC and CT plants run currently supported operating systems.	Moderate	Management respectfully requests considering including "Where technically feasible,…" to allow TVA to document exceptions where there is a concern of risk to operation by implementing the recommendation on a device/system.. Management agrees.
3	Ensure all servers and workstations in the gas secure rooms run currently supported operating systems.	Low	Management respectfully requests considering including "Where technically feasible,…" to allow TVA to document exceptions where there is a concern of risk to operation by implementing the recommendation on a device/system.. Management agrees.
4	Ensure all servers and workstations in the gas secure rooms are appropriately patched	Moderate	Management agrees.
5	Remove unneeded accounts from the servers and workstations in the gas secure rooms.	Low	Management agrees.
6	Define and implement baseline configurations for the servers and workstations in the gas secure rooms	Low	Management agrees.
7	Reevaluate the continued need for physical gas secure rooms.	Low	Management agrees.