State of Florida

Public Service Commission

CAPITAL CIRCLE OFFICE CENTER • 2540 SHUMARD OAK BOULEVARD
TALLAHASSEE, FLORIDA 32399-0850

-M-E-M-O-R-A-N-D-U-M-

DATE: April 29, 2025

JLAC received 4.28.25

TO: Mike La Rosa, Chairman

FROM: Valerie Peacock, Inspector General

RE: Six-month Follow-up of the Auditor General's Prior Audit Follow-Up of the Florida Public Service Commission (Report No. 2025-040)

Pursuant to Section 20.055(6)(h), Florida Statutes, the Office of Inspector General has conducted a six-month follow-up review of the status of the Commission's response to the finding and recommendation outlined in the Auditor General's Prior Audit Follow-Up (Report No 2025-040). The attached follow-up summary form provides the original finding and recommendation, the Commission's initial response, and summarizes actions taken within six months to address the finding.

If you have any questions or wish to discuss, please let me know.

Attachment

cc: Commissioner Gary F. Clark
Commissioner Andrew Giles Fay
Commissioner Art Graham
Commissioner Gabriella Passidomo-Smith

Legislative Joint Audit Committee

Braulio L. Baez
Apryl Lynn
Mark Futrell
Mary Anne Helton
Bobby Maddox

Florida Public Service Commission
Office of Inspector General
Prior Audit Follow-Up
Auditor General Report No. 2025-040

Auditing Entity	Report Number & Title	Final Report Issue Date	Summary of Findings and Recommendations	Summary of Corrective Actions Taken
Auditor General	2025-040 Prior Audit Follow-Up	October 2024	**Finding 1: Security Controls – Network User Authentication** Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to network user authentication need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Commission data and related IT resources. However, we have notified appropriate Commission management of the areas needing improvement. Without appropriate security controls related to network user authentication, the risk is increased that the confidentiality, integrity, and availability of Commission data and related IT resources may be compromised. A similar finding was communicated to Commission management in connection with our report No. 2022-063 (Finding 4). **Recommendation 1:** We again recommend that Commission management improve certain security controls related to network user authentication to ensure the confidentiality, integrity, and availability of Commission data and related IT resources. **Commission Response** The Commission agrees with the finding and is evaluating options to strengthen controls related to network user authentication as recommended.	**Actions Taken by Management at Six Month Follow Up**: **OIG Six-Month Follow Up Review** OIG verified that the Commission's Division of Administrative and IT Services (AIT) has worked to implement a nightly forced reboot of all network users. The Commission's multi-factor authentication (MFA) software does not provide for a mechanism to require users to be logged out after a set time. However, the system implemented force reboot requires staff to authenticate using MFA for daily login. This process was implemented on April 29, 2025. **6-Month Follow-up Results** The Commission has implemented process controls consistent with the requirements for MFA under Chapter 60GG-2, F.A.C., as referenced in the audit report.