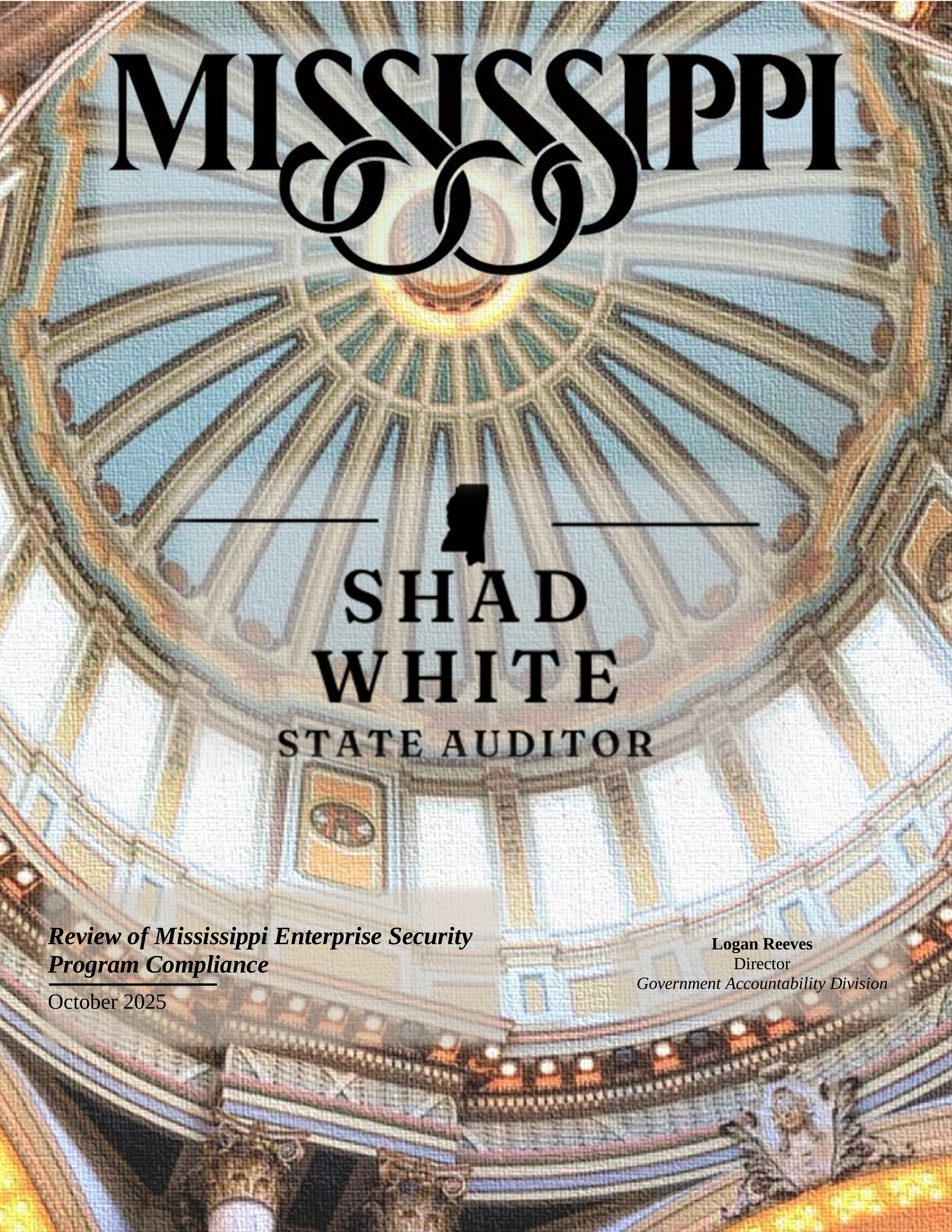


MISSISSIPPI

SHAD WHITE

STATE AUDITOR

Review of Mississippi Enterprise Security Program Compliance

October 2025

Logan Reeves
Director
Government Accountability Division

Executive Summary

Cybercrime now routinely threatens Mississippi taxpayers and government services. According to the FBI Internet Crime Report, 850,000 cybercrimes like phishing and ransomware attacks were reported in 2024.[1] Recently, Mississippi government offices have been victims of cybercrimes. For example:

- A 2023 ransomware attack on Hinds County disrupted government services and prevented citizens from registering vehicles or completing real estate transactions. The attack cost taxpayers at least $600,000 to resolve.[2]

- A data breach in late 2024 disrupted the Starkville-Oktibbeha Consolidated School District.[3]

- In July 2025, an online meeting of the Mississippi Opioid Settlement Fund Advisory Council, hosted by the Attorney General's office, was hacked.[4]

A 2019 survey conducted by the Office of the State Auditor (OSA) showed many Mississippi state agencies were not in compliance with the Mississippi Enterprise Security Program (ESP). At that time, 125 state agencies were surveyed to verify compliance, and 54 institutions chose not to respond. Further 65% of Mississippi state agencies either failed to report compliance or were out of compliance with the Enterprise Security Program.[5]

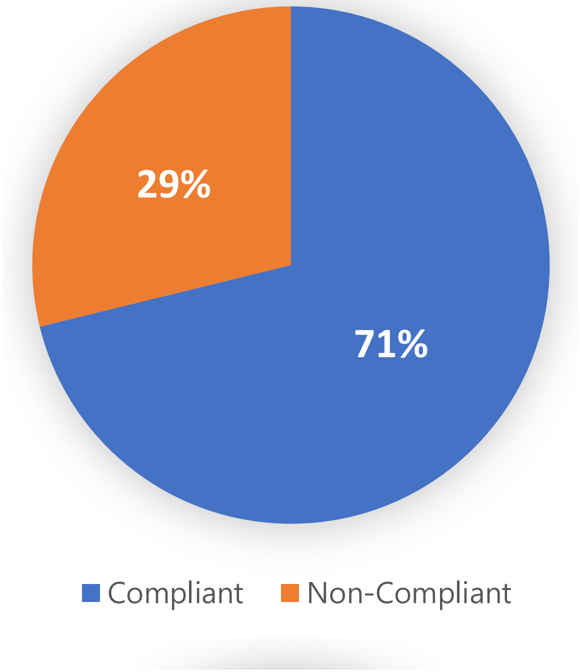
Key Finding: Today, nearly one third of state agencies have not met Mississippi's Enterprise Security Program requirement to conduct a comprehensive, third-party cybersecurity assessment. Failure to follow the state's cybersecurity program exposes critical government operations to unnecessary risk.

[1] See report.
[2] See article.
[3] See article.
[4] See article.
[5] See report.

Analysis

By law, state agencies must comply with the Enterprise Security Program which provides Mississippi state agencies with a unified approach to cybersecurity. The Mississippi Department of Information Technology Services (ITS) administers the Enterprise Security Program, and the Mississippi Office of the State Auditor monitors whether state agencies comply with the policy.[6] This year, the Auditor's office determined nearly one-third of government offices in Mississippi failed to comply with the ESP by not conducting a comprehensive third-party cybersecurity assessment. Figure 1 displays aggregated results of the analysis.

Figure 1



Of Mississippi's government agencies, 32 had not met the ESP's cybersecurity assessment requirements by September 8, 2025—a larger number of noncompliant agencies than in 2019. Ensuring proper policies and procedures are in place is one of the most important measures a government office can take to ensure proper cybersecurity controls. The government creates, stores, and maintains a wealth of personally identifiable information like health, tax, and student data. **Continued noncompliance with the ESP exposes that data to increased risk from potentially vulnerable state computer systems.**

[6] Mississippi Code §25-53-201

Conclusion

State government cybersecurity is a serious issue for Mississippi taxpayers and citizens. Mississippians deserve to know their personal information will be safe from cyber-attacks. The results of this analysis show government offices in Mississippi do not follow basic cybersecurity procedures. As a result, Mississippians' data or access to basic government services is at risk. **Leaders of state agencies should engage with IT professionals to ensure their agency complies with state law.** Finally, state leaders should continue to collaborate and share cybersecurity best practices for preventing security incidents.