NM DEPARTMENT OF INFORMATION TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor
Manny Barreras
Cabinet Secretary

TO: Office of the State Auditor

FROM: Jason L. Clack, General Counsel

DATE: March 17, 2026

SUBJECT: Public Comment Opposing Proposed SOC-2 and SOC-3 Requirements in Amendments to 2.2.2 NMAC (Audit Rule)

Introduction

DoIT is concerned that the Rule requiring SOC 2 and SOC 3 audits, NMAC 2.2.2.10(S), exceeds the statutory authority of the Office of State Auditor (OSA) and may introduce unnecessary risks for the state. The statutory mandate of OSA is to examine the financial affairs of state agencies by conducting audits in accordance with generally accepted auditing standards. Section 12-6-3(A) NMSA 1978.

SOC 2 and SOC 3 are Cybersecurity Audits not Financial Audits

SOC 1 and SOC 2 are two types of System and Organization Controls (SOC) audits designed to assess the internal controls of service organizations. While both are conducted by third-party auditors, they serve different purposes and target distinct audiences.

SOC 1 focuses on controls that impact a customer's financial reporting. It is typically required for organizations that handle financial transactions or data, such as payroll processors or payment service providers. The primary goal is to ensure that financial information is managed securely and accurately.

SOC 2, on the other hand, evaluates controls related to Trust Services Criteria (TSCs), which include security, confidentiality, availability, processing integrity, and privacy of customer data. It is more general and non-financial in nature and addresses a service organization's ability to protect sensitive data and maintain system reliability.

SOC 3 is similar to SOC 2 in terms of the criteria it covers but is designed for public disclosure. SOC 3 essentially provides a high-level summary of the SOC 2 audit, without revealing sensitive details. SOC 3 is often used in marketing materials to demonstrate a commitment to security while reserving the detailed SOC 2 report for clients who require in-depth information.

The OSA previously promulgated the Rule requiring the SOC 2 and SOC 3 audits based on the Statements on Auditing Standards 145 (SAS No. 145). SAS no. 145 enhances the

requirements and guidance on identifying and assessing the risks of material misstatement, in particular the areas of understanding the entity's system of internal control and assessing control risk. SAS no. 145 defines general IT controls as controls over the entity's IT processes that support the continued, proper operation of the IT environment, including the effective functioning of information-processing controls and the integrity of information in the entity's information system. It defines risks arising from the use of IT as susceptibility of information-processing controls to ineffective design or operation, or risks to the integrity of information due to ineffective design or operation of controls in the entity's IT processes. It requires auditors to identify general IT controls that address the risks arising from the use of IT and evaluate their design and implementation to ensure that controls support financial reporting and mitigate risk. The SAS no. 145 assessment is based on data quality controls in the IT environment, to ensure that data in financial reporting is accurate. These are the controls that are assessed in a SOC 1 audit not SOC 2 or SOC 3.

SOC 2 and SOC 3 have a much broader scope than what is required by SAS no. 145. SOC 2 is a cybersecurity framework that specifies how organizations should protect customer data from unauthorized access, security incidents, and other vulnerabilities. SOC 2 was designed to provide auditors with guidance for evaluating the operating effectiveness of a service provider organization's security protocols. SOC 2 refers to both the security framework and the audit that checks whether a company is compliant with SOC 2 requirements. SOC 2 reports focus on controls addressed by five semi-overlapping categories called "Trust Service Criteria" which are centered around the security of customer data, whereas SAS no. 145 requires assessment of IT controls to mitigate the risk or errors in financial reporting. SAS no. 145 does not support the justification of a Rule requiring a SOC 2 or SOC 3 audit.

The Cybersecurity Office, not OSA, has Statutory Authority to Set and Monitor Cybersecurity Controls

SOC 2 and SOC 3 are cybersecurity audits. The NM legislature has vested authority in the Cybersecurity Office, an administratively attached agency to DoIT, to "adopt and implement rules establishing minimum security standards and policies to protect agency information technology systems and infrastructure and provide appropriate governance and application of the standards and policies across information technology resources used by agencies to promote the availability, security and integrity of the information

processed, transacted or stored by agencies in the state's information technology infrastructure and systems," and "monitor agency information technology networks to detect security incidents and support mitigation efforts." Section 9-27A-3(B) NMSA 1978. It is therefore the authority of the Cybersecurity Office to set cybersecurity standards for agencies and monitor their compliance with those standards. By using SAS no. 145, which requires an assessment of IT controls to mitigate risks in financial reporting (SOC 1), to justify the requirement of a cybersecurity framework and audit of that framework (SOC 2 and SOC 3), the OSA is exceeding its statutory authority and encroaching upon the authority of the Cybersecurity Office.

DoIT is also concerned that publishing of design or effectiveness of controls in the SOC 3 may reveal information to malicious actors, which would enable them to infer unrelated control weaknesses using techniques, such as social engineering, to exploit security vulnerabilities.

Requested Revisions to the Proposed Rule

Based on the foregoing, the undersigned respectfully request that the Auditor's Office take the following actions regarding the proposed changes to the Audit Rule:

1. Rescind and delete existing §§ 2.2.2.7 (S)(2) – (4).
2. Do not adopt proposed §§ 2.2.2.10 (S)(2) – (14) or any requirement to initiate, perform, or publicly release a SOC-2 or SOC-3 report for the SHARE, DFA, or other state government systems.
3. Rescind and delete the definitions of "SOC-2" and "SOC-3" in §§ 2.2.2.7 (S)(4) – (5).
4. Delete the reference to "SOC 2" in § 2.2.2.14(D).

Conclusion

DoIT requests that any OSA requirements for SOC 2 and SOC 3 audits be withdrawn completely, as these requirements exceed the statutory authority of the OSA to examine the financial affairs of state agencies and encroaches on the statutory authority of the Cybersecurity Office and DoIT to monitor compliance with cybersecurity controls. These requirements also pose unnecessary risks to the state. Cybersecurity standards and compliance are maintained and monitored by the Cybersecurity Office and DoIT not the Office of the State Auditor.

NM DEPARTMENT OF
INFORMATION
TECHNOLOGY

Michelle Lujan Grisham
New Mexico Governor
Manny Barreras
Cabinet Secretary

Respectfully submitted,

Jason Clack

Jason L. Clack
General Counsel