New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

Date: March 2, 2026

To: Office of the State Auditor

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

Introduction

The undersigned, on behalf of their respective state agencies, firmly oppose the proposed amendments to the Audit Rule that would expand the Auditor's authority to mandate SOC-2 and SOC-3 audits of the Statewide Human Resources Accounting and Reporting Enterprise ("SHARE") system and the Department of Finance and Administration ("DFA").

These proposals exceed the Auditor's legal authority, conflict with the Department of Information Technology's jurisdiction, pose unacceptable, potentially uninsurable risks to the State's finances, and threaten to harm public employees, local public bodies, state vendors, and state retirees. By exceeding the statutory authority outlined in the Audit Act, the Audit Rule poses a clear and present danger to the security of data and the information technology infrastructure that supports the state's accounting for revenue, assets, and expenditures.

I. The Proposed Rule Conflicts with the Statutory Authority Granted to the Department of Information Technology.

New Mexico law prevents a state agency from expanding its rulemaking authority into areas already designated to other agencies by the legislature. Where statutes clearly define the exclusive jurisdictional boundaries among agencies, proposed rules must be supported by specific legal authority. *See* § 14-4-2, NMSA 1978.

The Auditor's Office intends to promulgate the proposed updates to § 2.2.2.10 (S) (3) – (14) through Statements on Auditing Standards 145 ("SAS No. 145"). SAS No. 145 defines general IT controls as controls over the entity's IT processes that ensure the proper operation of the IT environment, including the effectiveness of information-processing controls and the integrity of data within the entity's information system.

System and Organization Controls ("SOC") 2 and 3 engagements have a broader scope than 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. It was created by the American Institute of Certified Public Accountants ("AICPA") in 2010. SOC-2 was designed to provide auditors with guidance on evaluating the operating effectiveness of a service provider organization's security protocols.

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

SOC-2 pertains to both the security framework and the audit process that verifies a company's compliance with SOC-2 standards. These reports emphasize controls within five overlapping categories called “Trust Service Criteria,” primarily focusing on the security of customer data. In contrast, SAS no. 145 mandates the evaluation of IT controls to reduce errors in financial reporting. SOC-3 audit reports are derived from SOC-2 audits but exclude certain details and confidential information to make them suitable for public sharing.

SAS No. 145 does not justify a rule mandating SOC-2 or SOC-3 audits. SOC-2 and SOC-3 engagements are cybersecurity audits. The legislature has authorized the Cybersecurity Office of the Department of Information Technology (“DoIT”) to set security standards and monitor agency networks, as outlined in § 9-27A-3(B), NMSA 1978. The Cybersecurity Office, not the Auditor’s Office, has the authority to establish cybersecurity standards for agencies and oversee agency compliance with these standards. The Auditor’s Office is overstepping its statutory authority by bootstrapping its proposed updates to § 2.2.2.10 using SAS No. 145. SAS No. 145 requires an assessment of IT controls for financial reporting risks; this does not justify or authorize the Auditor’s Office to establish a cybersecurity framework for state systems and audit standards for this framework. This shifts authority away from the Cybersecurity Office and to the Auditor’s Office, in direct conflict with § 9-27A-3 (B), NMSA 1978.

Given the statutory authority granted to DoIT, encroachment by the Auditor’s Office into this area is both ill-advised and in direct violation of the legislature’s intent.

II. The Auditor Lacks Authority Under Section 12-6-3(C), NMSA 1978, to Require Non-Financial Audits by Rule.

New Mexico courts have consistently held that agencies may not exceed their statutory rulemaking limits. In *Stapleton v. Skandera*, the Court of Appeals clarified that "[a]gencies are created by statute, and are limited to the power and authority expressly granted or necessarily implied by those statutes." *See State ex rel. Stapleton v. Skandera*, 346 P.3d 1191 (N.M. App. 2015). The court emphasized that "the administrative agency's discretion may not justify altering, modifying, or extending the reach of a law created by the Legislature." *See State ex rel. Stapleton v. Skandera*, 346 P.3d 1191, (N.M. App. 2015).

The New Mexico Supreme Court reinforced these limitations in *Rivas v. Board of Cosmetologists*, holding that "[a]n administrative agency has no power to create a rule or regulation that is not in harmony with its statutory authority." *See Rivas v. Board of Cosmetologists*, 101 N.M. 592 (1984). The practical effect of these limitations is that agency rules exceeding statutory authority are "unenforceable" and constitute "a nullity." *See Rivas v. Board of Cosmetologists*, 101 N.M. 592 (1984).

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

The Audit Act (§ 12-6-1 et seq., NMSA 1978) authorizes the State Auditor, in addition to annual audits, to conduct financial examinations and audits of the financial affairs and transactions of state agencies. See § 12-6-3 (C), NMSA 1978. While the term financial affairs and transactions is not defined in the Audit Act, the AICPA defines "financial affairs and transactions" to refer to economic activities, interests, and exchanges. Moreover, under § 2.2.2.15 (B), NMAC, the Auditor's Office limits its authority to conduct special audits or examinations to engagements that address financial fraud, waste, or abuse in government.

Unfortunately, the proposed updates to § 2.2.2.10 (S) (3) – (14) NMAC seem to ignore these limitations and establish standards for SOC-2 and SOC-2 engagements. The proposed changes aim to mandate DFA engage in SOC-2 and SOC-3 audits of the SHARE system and its internal segregation of duties. However, as established above, SOC-2 and SOC-3 are not financial audits. They do not review financial transactions or transactions of a state agency, as required by § 12-6-3(C), NMSA 1978.

The Audit Rule describes SOC-2 as an audit that provides an opinion on controls related to security, availability, processing integrity, confidentiality, or privacy at the service organization, helping users evaluate their internal controls. See § 2.2.2.7 (S) (4), NMAC. Similarly, SOC-3 is defined as an audit that provides an opinion on the effectiveness of controls relevant to security, availability, processing integrity, confidentiality, or privacy at the service organization. See § 2.2.2.7 (S) (5), NMAC. Consequently, neither definition appears to align with the express limitation in §§ 2.2.2.7 (S) (6) or 2.2.2.15 (B) for special audits. According to the Audit Rules' definitions, neither SOC-2 nor SOC-3 audits examine the financial activities of SHARE or DFA, nor are they intended to detect financial fraud, waste, or abuse in SHARE or DFA's functions.

Under § 12-6-3(C), NMSA 1978, and § 2.2.2.15 (B) of the NMAC, the Auditor lacks the authority to mandate SOC-2 or SOC-3 audits. The Auditor's power to order special audits is limited to those addressing financial fraud, waste, or abuse in government. Because SOC-2 and SOC-3 audits evaluate IT controls related to security, availability, processing integrity, confidentiality, and privacy, and do not assess an agency's financial transactions, they fall outside the scope of audits the State Auditor can require under the Audit Act.

Given the express limitations in the Audit Act and Audit Rule, the proposed changes to § 2.2.2.10 (S) (3) – (14) expand the Auditor's authority to conduct special audits in violation of the Rivas cases' holding, rendering them ultra vires, unenforceable, and a nullity if adopted.

III. The Proposed Rule Creates an Unacceptable and Uninsurable Risk to the State's Financial System.

In addition to the lack of statutory authority and encroachment on another agency's statutory authority, the proposed changes to § 2.2.2.10 (S) (3) – (14), if adopted, will create an uninsurable liability risk for the state, potentially exceeding the current value of the state's public liability fund. In

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

general, SOC-2 reports provide detailed descriptions of system architecture, control design, and potential vulnerabilities. SOC-3 reports are derived from SOC-2.

The SHARE system stores federally protected PII, payroll data, employee and vendor banking information, and tax identification numbers. It is a highly customized IT infrastructure with complex integrations and access points. Public release of a SOC-2 or SOC-3 report covering the system's architecture, control design, and potential vulnerabilities would expose sensitive security information to malicious actors, including 24,000 state employees, 50,000 vendors, and New Mexico taxpayers. Moreover, this requirement conflicts with the exemption in the Inspection of Public Records Act for sensitive IT security information. See § 14-2-1(J), NMSA 1978. Given the system's complexity and sensitivity, issuing a public report on its architecture, control design, and potential vulnerabilities could inadvertently disclose confidential security findings, exposing state agencies, employees, vendors, and citizens to risk.

Such disclosure could result in significant liability for the state. The SHARE system processes approximately $26 billion in transactions annually. Under § 41-4-23, the legislature created the Public Liability Fund to insure state agencies and local public bodies against liabilities. The fund is designed to defend and indemnify these entities and their employees for claims covered by valid insurance certificates, up to the policy limits. However, the fund is not capitalized to absorb billions of dollars in claims arising from the release of a public audit report detailing the SHARE system's architecture, control design, and potential vulnerabilities. In such a case, legislative action would be needed to address claims linked to this disclosure.

Furthermore, SOC-2 and SOC-3 audits are also known as "Service Organization Control" 2 and 3 engagements because they generally relate to service organizations. A service organization is an external entity that offers information systems as a service to other organizations. These organizations outsource vital services, including payroll, data centers, cloud computing, and software-as-a-service. Service organizations publishing SOC-3 audits for their systems are vendors selling services to third parties. DFA is part of the user entity of the SHARE system, the New Mexico government. Generally, user entities are not subject to the trust service criteria of SOC-2 or SOC-3 audits. Although DFA maintains the SHARE system on behalf of the New Mexico state government, it would not be classified as a service organization under the SOC standards.

Additionally, the public nature of a SOC-3 report conflicts with the security, confidentiality, and risk-management standards required to protect sensitive government infrastructure, such as the SHARE system. While a SOC-3 audit may demonstrate a broad commitment to security, its primary purpose is to serve as a marketing tool for third parties. It lacks the detailed control descriptions and testing results that security-sensitive government stakeholders need to evaluate a system. Because DFA neither promotes nor sells the SHARE system or its capabilities externally (state agencies are required by statute to use it, and DFA is required to maintain it), releasing a

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

SOC-3 audit for SHARE would provide no public benefit and would significantly increase the state's cybersecurity risk and liability.

IV. 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. Delete § 2.2.2.7 (S) (4) – (5).
2. Delete § 2.2.2.10 (S) (2) – (14) and any requirement to initiate, perform, or publicly release a SOC-2 or SOC-3 report for the SHARE or DFA systems.
3. Rescind all disqualifications issued to audit firms by the Office of State Auditor, prohibiting firm(s) from performing SOC-2 audits in the state.
4. Clarify that SOC-2 and SOC-3 engagements are not mandated under the Audit Act and are outside OSA's rulemaking authority under § 12-6-12, NMSA 1978, as they do not concern financial affairs and transactions.
5. Avoid imposing SOC-based requirements that conflict with DoIT's statutory authority to set cybersecurity standards and monitor compliance.

Conclusion

For the reasons stated above—the absence of statutory authority under § 12-6-3(C) for non-financial IT audits, the conflict with DoIT's cybersecurity authority, and the unacceptable risk posed by public SOC-3 reporting—the proposed SOC-2/SOC-3 requirements should be withdrawn consistent with these comments. The proposed changes § 2.2.2.10 (S) (2) – (14) pose a clear and present risk to the security of data and the information technology infrastructure supporting the state's accounting for revenue, assets, and expenditures.

Regards,

Signed by:
George Hypolite
8F9C3BE14553478...

George Hypolite
General Counsel
New Mexico Department of Finance and Administration

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

The following state agencies have reviewed the analysis, oppose adopting the SOC-2 and SOC-3 requirements in the proposed rule, and support the requested revisions.

Signed by:
Craig Hay
4953EE916CE2472...
Craig Hay
Acting General Counsel
New Mexico Aging and Long-Term Services Department

Signed by:
Julie Sakura
6AD37C3ED66B4AD...
Julie Sakura
General Counsel
New Mexico Department of Health

DocuSigned by:
Mark Lovato
CEBD5E8873E2477...
Mark Lovato
General Counsel
New Mexico Corrections Department

Signed by:
Kevin A Graham
C6C54A5F586343C...
Kevin A. Graham
Chief General Counsel
New Mexico Regulation and Licensing Department

DocuSigned by:
Todd Baran
79BDD89BB105451...
Todd Baran
General Counsel
New Mexico Office of Cyber Security

Signed by:
Joseph Holloway
E7843D94CE784A6...
Joseph Hollaway, Esq.
Deputy Director
Expo New Mexico

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

DocuSigned by:
CHRIS MACHIN
960EFA3078E24FF...
Chris Machin
General Counsel
New Mexico Livestock Board

Signed by:
Rose Bryan
DBBEEDEDFC9D431...
Rose Bryan
Chief General Counsel
New Mexico Health Care Authority

Signed by:
AdelinaGomez
3DBD15AEC2BE45C...
Adelina Gomez
General Counsel
New Mexico Indian Affairs Department

DocuSigned by:
Nat Chakeres
FBDB431E8E634E7...
Nathaniel Chakeres
General Counsel
New Mexico Office of State Engineer

DocuSigned by:
Jeremy Ian Martin
398087C7ED434FC...
Jeremy Ian Martin
Chief General Counsel
New Mexico Department of Game and Fish

DocuSigned by:
Cassandra Brulotte
C0140201B6F94E1...
Cass Brulotte
General Counsel
New Mexico Office of Broadband Access and Expansion

New Mexico
Department of Finance
and Administration

407 Galisteo St,
Santa Fe, NM 87501
(505) 827-4985

Cabinet Secretary Wayne Propst

Governor Michelle Lujan Grisham

DocuSigned by:
Leigh Messerer
2AA1D7C988D3401...
Leigh Messerer
General Counsel
New Mexico State Personnel Office

DocuSigned by:
Jason Clack
8A978A90D5EA400...
Jason Clack
General Counsel
New Mexico Department of Information Technology

Signed by:
Alexis Johnson
3EF8223ABD5D434...
Alexis Johnson
Acting General Counsel
New Mexico General Services Department