New Mexico
Department *of* Finance
and Administration

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

Cabinet Secretary Wayne Propst
Deputy Cabinet Secretary Renee Ward
Acting State Controller Mark Melhoff

Governor Michelle Lujan Grisham

To: Joseph Maestas, *State Auditor*
New Mexico Office of the State Auditor
Joseph.Maestas@osa.nm.gov

From: Mark Melhoff, *Acting State Controller*, Financial Control Division
New Mexico Department of Finance and Administration

Date: April 25, 2025

RE: PUBLIC COMMENT REGARDING 2025 PROPOSED CHANGES TO THE NEW MEXICO STATE AUDIT RULE

This memorandum shall serve as public comment by the Financial Control Division ("FCD") of the Department of Finance and Administration ("DFA") regarding proposed changes to the 2025 Audit Rules under the New Mexico Administrative Code ("NMAC"). The FCD's public comments are as follows.

The DFA strongly opposes the proposed changes to the audit rule requiring an SOC-3 audit report for the SHARE system.

DFA expresses its opposition to the proposed amendments to NMAC 2.2.2.10.S.2, which mandate DFA submit a SOC-3 SHARE report to the state auditor for publication. Initially, DFA articulates its specific disagreement with the definition of a SOC-3 audit report as outlined in NMAC 2.2.2.10.S.2.

By definition, a SOC-2 audit evaluates an organization's controls related to data security, availability, processing integrity, confidentiality, and privacy. A SOC-3 audit report provides a public overview of these controls. However, both audits and reports address vulnerabilities related to these five Trust Services Criteria ("TSC").

A SOC-2 audit report requires an in-depth assessment of internal controls, including:

- **Security:** Focuses on preventing unauthorized access, misuse, data deletion, or disruption of services. This includes testing firewalls, intrusion detection systems, access controls, encryption, and antivirus software.
- **Availability:** Ensures systems are accessible to users when needed, including backup and recovery processes.
- **Processing Integrity:** Tests the accuracy, completeness, and reliability of data processing.
- **Confidentiality:** Focuses on preventing unauthorized disclosure of sensitive information.

- **Privacy:** Ensures compliance with privacy laws and regulations related to data handling.

A SOC-3 audit report requires a public assurance determination of internal controls, including:

- **Security:** Provides a public overview of the organization's security controls.
- **Availability:** Describes the organization's controls for ensuring system availability.
- **Processing Integrity:** Summarizes the organization's controls for accurate data processing.
- **Confidentiality:** Outlines the organization's controls for protecting sensitive information.
- **Privacy:** Provides a public overview of the organization's data privacy practices.

NMAC 2.2.2.10.S.2's definition of a SOC-3 audit report assumes that a SOC-2 audit report can simply be redacted to generate a SOC-3 audit report that the auditor may make public. However, creating a SOC-3 report is not as straightforward as redacting a SOC-2 audit report. Generally, due to the nature of the SHARE system, a SOC-2 audit requires a thorough examination of DFA/SHARE's internal controls, accompanied by detailed testing results to ensure sufficiency. A SOC-3 audit is typically regarded as inappropriate for scenarios where detailed internal control information and specific test results are necessary, given the high complexity of the SHARE system and specific regulatory requirements for the system.

Additionally, publishing a SOC-3 audit report will increase the cybersecurity risks to the SHARE system, leading to the disclosure of valuable information to actors seeking to exploit the financial data contained in the SHARE system. A public report detailing the SHARE system's TSC internal controls will lead to:

1. **Unauthorized Access.** A SOC-3 audit report will provide an overview of SHARE's internal security controls and practices. Malicious actors could use this information to identify vulnerabilities and exploit them.

2. **Misuse of Controls.** Malicious actors could use the descriptions and summaries of SHARE's controls for accurate data processing and system availability in a SOC-3 audit report to bypass and manipulate security controls and access SHARE.

3. **Insider Threats.** Malicious actors could combine the information in the SOC-3 report with other types of general system attacks to facilitate malicious activities such as data theft or sabotage.

4. **Information Disclosure.** An SOC-3 report will contain sensitive information about SHARE's security posture, confidentiality controls protecting sensitive information, and privacy practices.

5. **Legal Consequences.** If a compromised SOC-3 report causes a data breach or other security incidents, the state may face legal liability and possible regulatory consequences, depending on the data compromised.

Additionally, the FCD asserts that the publication of NMAC 2.2.2.10.S.2's SHARE SOC-3 audit report is at odds with the legislative intent and DFA's obligations under the Inspection of Public Records Act, specifically §14-2-1 (J), NMSA 1978. This statute clearly exempts from public inspection "information concerning information technology systems, the publication of which would reveal specific vulnerabilities that compromise or allow unlawful access to such systems." While the exemption does not outright ban requests for external audits of information technology systems, it does prevent the release of any segments that would disclose ongoing vulnerabilities that may compromise or enable unlawful access to such systems. As outlined above, given the nature of the SHARE system, a SOC-3 audit report is typically deemed unsuitable for systems like SHARE because SHARE's SOC-2 audit necessitates a comprehensive review of SHARE's internal controls, along with detailed testing results to confirm their adequacy. Consequently, any description or summary of SHARE's TSC internal controls will expose ongoing vulnerabilities that could compromise or facilitate unlawful access to SHARE.

Finally, there is no legal, federal, or statutory requirement to provide a SOC-3 audit report for SHARE. DFA strongly opposes this rule change and believes it would put confidential employee and vendor/supplier data at risk, in contradiction with § 14-2-1 (J). I ask that you consider striking the SOC-3 requirement and allowing the state to continue safeguarding employee and vendor data.

The FCD proposes changes to the report due dates under NMAC 2.2.2.9.A.1.C.

Under NMAC 2.2.2.9.A.1.C, the due date for DFA's agency audit is November 1st. FCD proposes changing the date for DFA-341 to November 15th for the following reason. DFA houses the Board of Finance's severance tax bond ("STB") Capital Outlay program, which provides funds for all legislatively approved STB capital outlay projects. Collecting and testing data and controls for such a wide-ranging program adds complexity and time to the completion of the DFA's agency audit. DFA must complete its audit by November 1st while relying on other state agencies to perform reconciliation and close out prior years' activities in a timely manner. If due dates continue to be extended for other state agencies, DFA recommends providing a corresponding extension for DFA's agency audit.

The FCD proposes changes to the exit conference and related confidentiality issues under NMAC 2.2.2.10.M.3.

Under NMAC 2.2.2.10.M.3, the agency and IPA are permitted to provide the Controller's Office with draft financial statements and notes, but they are prohibited from sharing the opinion and findings with the Controller's Office until released by OSA. The exclusion of the State Controller's Office from the initial opinion and findings can result in a delay in completing the State ACFR as required by § NMSA 1978, 6-5-4.1. Additionally, as the state's accounting oversight body, the Controller's Office "must have access to and authority to examine books, accounts, reports, voucher" to properly monitor and oversee state agencies and ensure compliance with state and federal law pursuant to § NMSA 1978, 6-5-2.1 (S). Please consider including DFA in the initial submission phase of an agency audit to encompass the opinion and findings.

The State Controller's Office of the DFA proposes additional notice requirements to the Report Due Dates under NMAC 2.2.2.9.A.5.

FCD suggests that the DFA be listed as an agency that must be notified when there are circumstances that will delay an agency's audit report. DFA is tasked with preparing the State's ACFR, which relies heavily on the timely submission of audits from state agencies. Delays in audits submitted by a state agency, entity, or component entity extend the time required to compile the ACFR accurately. Therefore, the Controller respectfully requests that DFA, similar to the state auditor, be informed of any situations that might cause an agency's audit report to be late, as long as the state entity is under the DFA's jurisdiction and reports within the ACFR.

Additionally, the Secretary of Finance and Administration is required to order monthly financial reporting by any entity that has not submitted its annual audit pursuant to § NMSA 1978, 9-6-5.2 (A). Requiring late notices to be sent to both OSA and DFA would ensure that DFA is able to effectively enforce this statutory obligation and assist OSA in ensuring compliance with reporting requirements.

For questions, email the Acting State Controller, Mark Melhoff at marks.melhoff@dfa.nm.gov.