OFFICIAL STATE CABINET AGENCY RESPONSE TO PERFORMANCE AUDIT ON SAFE DATA DISPOSAL: STATE REDUCES THE RISK OF DISCLOSING CONFIDENTIAL INFORMATION – DECEMBER 13, 2018

This management response to the State Auditor's Office (SAO) performance audit report received November 20, 2018, is provided by the Office of Financial Management and the Office of the Chief Information Officer (OCIO) on behalf of the audited agencies.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to answer this question:

1. Does the state have adequate controls in place to ensure that the surplus of state-owned IT devices does not disclose confidential data?

SAO Recommendation 1: Confidential management letters were sent to each of the 20 agencies that had their policies and procedures reviewed. These letters contained detailed information about how to better comply with state laws related to data disposal, as well as OCIO requirements and NIST best practices. We recommend these agencies review and address the issues described in those letters.

STATE RESPONSE: We appreciate the detailed information to help agencies improve their data disposal practices. Some agencies have already made improvements. Some of the updates to policies and procedures were underway before the audit began based on updates to OCIO Standard No. 141.10 in November 2017, pending approval of the Technology Services Board. Section 8.3 of this standard relates to media handling and disposal and it includes the National Institute of Standards and Technology (NIST) media sanitation guidelines referenced in the report for best practices. All state agencies who received a management letter should review these standards to address the issues described.

Action Steps and Time Frame

- Agencies who received a management letter will develop a timeline to address remaining issues to meet state requirements, as well as risk and complexity in their IT environment. *By March 31, 2019.*

SAO Guidance to all state agencies: The SAO also provided guidance to all state agencies because they consider the audit results so broadly applicable. They suggest that all state agencies consider these practices as they process surplused IT equipment:

- Annually review policies and procedures, and revise them as necessary to ensure they include the following state requirements and NIST best practices:
  - Designating management responsibility for the disposal of IT devices
  - Maintaining records of disposed equipment
  - Documenting the date equipment was sanitized, the method used and the name and signature of the person responsible
  - Keeping disposal records secure from unauthorized access
  - Sanitizing equipment using a method consistent with NIST guidelines
  - Verifying equipment is fully sanitized
  - Keeping equipment secure before and during sanitization
  - Physically destroying storage media if sanitization tools fail
- Update policies and procedures to include state-approved methods for erasing data from mobile devices such as cellphones and tablets.

Action Steps and Time Frame

- Not applicable.