OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON CONTINUING OPPORTUNITIES TO IMPROVE STATE IT SECURITY – JAN. 23, 2020

This management response to the State Auditor's Office (SAO) performance audit report received January 2, 2020, is provided by the State's Chief Information Officer on behalf of the audited agencies.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to answer this question:

1. Can selected agencies make their IT systems more secure, and better align their IT security practices with leading practices?

SAO Recommendations to the four selected state agencies: to help strengthen IT security programs, and to protect agency systems and the information within those systems, we recommend:

1. Continue remediating vulnerabilities identified during the security testing, starting with those that most significantly affect the agencies.
2. Consider further aligning agency IT security programs with leading practices recommended in the *Center for Internet Security (CIS) Controls*.
3. Identify and continue to periodically assess the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.

STATE RESPONSE:
Agencies embrace their responsibility to continuously improve State IT security. We agree with the opportunities for improvement identified by the SAO to strengthen IT security and are committed to ongoing assessment and improvement. The audited agencies have already made improvements and will continue to work diligently to address the findings. Agencies will also consider further aligning IT security programs with the leading practices recommended in the CIS Controls. To leverage leading practices, the Office of Cybersecurity will use the findings and observations of this audit to work with all state agencies to better improve the state's security posture.

Action Steps and Time Frame

‣ Each audited agency will establish a timeline to address vulnerabilities, improvements and considerations identified. *By March 31, 2020*.