OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON CONTINUING OPPORTUNITIES TO IMPROVE STATE IT SECURITY – 2018 DEC. 14, 2018

This management response to the State Auditor's Office (SAO) performance audit report received December 3, 2018, 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 state requirements and leading practices?

SAO Recommendations 1-4 to the three selected state agencies:

1. Continue remediating issues identified during security testing
2. Continue remediating gaps between agency IT security implementation or written policies and the procedures and the state's IT security standards
3. Consider also further aligning agency IT security controls with leading practices recommended in Critical Security Controls #1 through #5 and #11
4. Continue periodically assessing IT needs and resources, including personnel and technology, to develop and maintain sufficient IT security

STATE RESPONSE:
Agencies are committed to ongoing assessment and improvement of IT security needs. We agree with the opportunities for improvement identified to strengthen IT security by the SAO. The audited agencies will continue to work diligently to remediate the gaps identified between agency IT security implementation or written policies and procedures and the state's IT security standards. Agencies will also consider further aligning IT security controls with the leading practices the SAO identified.

Action Steps and Time Frame

- Each audited agency will establish a timeline to address the gaps, improvements and considerations identified. *By March 31, 2019*.

SAO Recommendation 5-7 to the Office of Cyber Security, WaTech:

5. Continue to reach out to state agencies to identify what information would help agencies:
    - Incorporate detailed controls into their policies and procedures
    - Align agency practices with the state IT security standards
6. Continue to develop and provide that additional clarity or guidance to state agencies
7. Continue to assess resources to better assist agencies in developing and implementing their IT security programs.

STATE RESPONSE:

The state Office of Cyber Security will survey state agencies to identify areas of security policy where agencies need additional clarification or interpretation in order to focus ongoing education and training programs.

OCS will use information from the survey to identify topics that will be addressed during its monthly technical and policy training sessions. In addition, OCS will prepare handouts to address frequently asked policy questions that can be provided to IT security staff by email, or when they visit OCS during weekly open office hours. OCS makes all staff available every Tuesday morning between 9:00 a.m. to Noon to address security questions and other issues. No appointment is necessary.

Action Steps and Time Frame

- OCS will survey state agencies and analyze the information collected to focus its education efforts. *By March 31, 2019*
- OCS will use the survey information during its ongoing outreach in order to help agencies incorporate detailed controls into their policies and procedures, and align agency practices with the state IT security standards. *By June 30, 2019*
- OCS will prepare explanatory handouts and continue to develop and provide that additional clarity or guidance to state agencies *Ongoing.*
- OCS will continue to assess resources to better assist agencies in developing and implementing their IT security programs. *Ongoing.*