OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON DATA BACKUP AND DISASTER RECOVERY – 2020, SEPT. 15, 2020

The State's Chief Information Officer on behalf of the audited agencies provides this management response to the State Auditor's Office (SAO) performance audit report received Aug. 13, 2020.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to answer these questions:

1. Have selected state agencies implemented data and system backup policies and procedures that comply with state requirements and align with leading practices?
2. Do the selected state agencies have a current, tested, disaster recovery plan that complies with state requirements and aligns with leading practices?

SAO Recommendations to the four selected state agencies: To reduce the risk of not being able to restore critical systems and data in the event of a disaster or malicious attack, we recommend the following:

1. Agencies perform and use IT risk assessments and business impact analyses to identify gaps in current backup and disaster recovery practices and procedures, recovery time objectives, and recovery priorities.
2. Executive management consider the results of these analyses and work closely with IT staff to ensure adequate resources are allocated to design and implement comprehensive backup and disaster recovery practices and procedures.
3. Agencies further align backup and disaster recovery practices and procedures with state requirements and leading practices.

STATE RESPONSE: We agree with the opportunities for improvement identified by the SAO and will continue to work diligently to remediate the issues identified. We are committed to ongoing assessment and improvement of backup and disaster recovery programs, as well as constructive communication and collaboration between agencies and those providing guidance and policy. Agencies need clear direction and timelines to effectively plan, improve and ensure resources as technologies evolve.

Where feasible, we will further align data backup and disaster recovery processes with the leading practices recommended in the CIS Controls, NIST Special Publication, and FISCAM.

The following action steps in response to the performance audit recommendations will support efforts to improve and maintain our data backup and disaster recovery plans.

Action Steps and Time Frame

- Audited agencies will establish a cadence for reviewing state requirements and leading practices and improving alignment where feasible. *By December 31, 2020.*
- Agencies will coordinate and gather business unit and technical interdependencies to conduct a business impact analyses through the Interagency Continuity of Operations Planning (iCOOP) Committee, beginning March 1, 2021. We estimate this process to take up to a year. *By March 31, 2022*.
- Audited agencies will conduct an IT risk assessment and business impact analyses. *By March 30, 2022*.
- Audited agencies' executive management (after completion and analysis of the IT Risk Assessment) will consider the results, risks, and resources assigned toward design, implementation and improvement of comprehensive backup routines. *By October 31, 2022.*
- Audited agencies' executive management (after completion and analysis of the IT Risk Assessment) will consider the results, risks, and resources assigned toward design, implementation and improvement of comprehensive disaster recovery routines. *By October 31, 2022.*

SAO Recommendations to the Office of the Chief Information Officer: To improve the ability of state agencies to comply with Standard 141.10 concerning data backup and Policy 151 concerning disaster recovery planning, we recommend the OCIO:

4. Update the IT Disaster Recovery and Business Resumption Guidelines and make them readily available to state agencies via the ocio.wa.gov website.
5. Offer agencies tools and templates for backup strategies and disaster recovery planning, such as IT Risk Assessments and Business Impact Analyses.

STATE RESPONSE: The OCIO agrees with the opportunities for improvement identified by the SAO and will work with other stakeholders to update guidelines and identify tools and templates to better assist agencies. The OCIO will coordinate with the Emergency Management Division of the Military Department who, through the iCOOP, is responsible for disseminating Continuity of Operations Planning (COOP) guidance to state agencies on methods of aligning to standards.

Action Steps and Time Frame

- OCIO will convene a workgroup with Military Department, Office of Cybersecurity (OCS), OCIO and agency Subject Matter Experts (SMEs) to evaluate updates to guidelines and identification of tools and templates. *By September 30, 2021*.
- The OCIO with the assistance of the workgroup will publish guidelines, tools and templates. B*y March 31, 2022.*
