uniform technology policies, standards, and procedures for use by executive branch agencies in implementing zero trust architecture and multi-factor authentication on all systems in accordance with this section.

(b) On or before July 1, 2024, the division shall **Ŝ→ [~~adopt~~] consider adopting ←Ŝ** the enterprise security practices described in this section and **Ŝ→ [~~implement~~] consider implementing ←Ŝ** zero trust architecture and robust identity management practices, including:

(i) multi-factor authentication;

(ii) cloud-based enterprise endpoint detection and response solutions to promote real-time detection, and rapid investigation and remediation capabilities; and

(iii) robust logging practices to provide adequate data to support security investigations and proactive threat hunting.

(4) (a) **Ŝ→ [~~In~~] If ←Ŝ** implementing a zero trust architecture and multi-factor authentication, the division shall **Ŝ→ [~~prioritize~~] consider prioritizing ←Ŝ** the use of third-party cloud computing solutions that meet or exceed industry standards.

(b) The division shall **Ŝ→ [~~give~~] consider giving ←Ŝ** preference to zero trust architecture solutions that comply with, are authorized by, or align to applicable federal guidelines, programs, and frameworks, including:

(i) the Federal Risk and Authorization Management Program;

(ii) the Continuous Diagnostics and Mitigation Program; and

(iii) guidance and frameworks from the National Institute of Standards and Technology.

(5) (a) In procuring third-party cloud computing solutions, the division may utilize established purchasing vehicles, including cooperative purchasing contracts and federal supply contracts, to facilitate efficient purchasing.

(b) The chief information officer shall establish a list of approved vendors that are authorized to provide zero trust architecture to governmental entities in the state.

(c) If an executive branch agency determines that procurement of a third-party cloud computing solution is not feasible, the executive branch agency shall provide a written explanation to the division of the reasons that a cloud computing solution is not feasible, including:

(i) the reasons why the executive branch agency determined that a third-party cloud computing solution is not feasible;

(ii) specific challenges or difficulties of migrating existing solutions to a cloud environment; and

(iii) the total expected cost of ownership of existing or alternative solutions compared to a cloud computing solution.

(6) (a) On or before November 30 of each year, the chief information officer shall report on the progress of implementing zero trust architecture and multi-factor authentication to:

(i) the **Ŝ→ [~~Government Operations~~] Public Utilities, Energy, and Technology ←Ŝ** Interim Committee; and

(ii) the Cybersecurity Commission created in Section 63C-25-201.

(b) The report described in Subsection (6)(a) may include information on:

(i) applicable guidance issued by the United States Cybersecurity and Infrastructure Security Agency; and

(ii) the progress of the division, executive branch agencies, and governmental entities with respect to:

(A) shifting away from a paradigm of trusted networks toward implementation of security controls based on a presumption of compromise;

(B) implementing principles of least privilege in administering information security programs;

(C) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(D) identifying incidents quickly; and

(E) isolating and removing unauthorized entities from agency systems as quickly as practicable, accounting for cyber threat intelligence or law enforcement purposes.