1   # CYBERSECURITY INFRASTRUCTURE MODIFICATIONS

2   ## 2023 GENERAL SESSION

3   ## STATE OF UTAH

4   **Chief Sponsor: Jon Hawkins**

5   Senate Sponsor: Daniel McCay

6   ==

7   **LONG TITLE**

8   **General Description:**

9   This bill enacts certain cybersecurity requirements for state information architecture.

10   **Highlighted Provisions:**

11   This bill:

12   ‣   defines terms;

13   ‣   specifies the applicability of the provisions enacted in this bill;

14   ‣   enacts requirements regarding the adoption of zero trust architecture and

15   multi-factor authentication for executive branch agencies; and

16   ‣   creates a reporting requirement.

17   **Money Appropriated in this Bill:**

18   None

19   **Other Special Clauses:**

20   None

21   **Utah Code Sections Affected:**

22   ENACTS:

23   **63A-16-214**, Utah Code Annotated 1953

24   ==

25   *Be it enacted by the Legislature of the state of Utah:*

26   Section 1. Section **63A-16-214** is enacted to read:

27   <u>**63A-16-214. Zero trust architectures -- Implementation -- Requirements --**</u>

28   **Reporting.**

29   (1) As used in this section:

30   (a) "Endpoint detection and response" means a cybersecurity solution that continuously

31   monitors end-user devices to detect and respond to cyber threats.

32   (b) "Governmental entity" means:

33   (i) the state;

34   (ii) a political subdivision of the state; and

35   (iii) an entity created by the state or a political subdivision of the state, including an

36   agency, board, bureau, commission, committee, department, division, institution,

37   instrumentality, or office.

38   (c) "Multi-factor authentication" means using two or more different types of

39   identification factors to authenticate a user's identity for the purpose of accessing systems and

40   data, which may include:

41   (i) knowledge-based factors, which require the user to provide information that only

42   the user knows, such as a password or personal identification number;

43   (ii) possession-based factors, which require the user to have a physical item that only

44   the user possesses, such as a security token, key fob, subscriber identity module card or smart

45   phone application; or

46   (iii) inherence-based credentials, which require the user to demonstrate specific known

47   biological traits attributable only to the user, such as fingerprints or facial recognition.

48   (d) "Zero trust architecture" means a security model, a set of system design principles,

49   and a coordinated cybersecurity and system management strategy that employs continuous

50   monitoring, risk-based access controls, secure identity and access management practices, and

51   system security automation techniques to address the cybersecurity risk from threats inside and

52   outside traditional network boundaries.

53   (2) This section applies to:

54   (a) all systems and data owned, managed, maintained, or utilized by or on behalf of an

55   executive branch agency to access state systems or data; and

56   (b) all hardware, software, internal systems, and essential third-party software,

57   including for on-premises, cloud, and hybrid environments.

58   (3) (a) On or before November 1, 2023, the chief information officer shall develop

59 uniform technology policies, standards, and procedures for use by executive branch agencies in
60 implementing zero trust architecture and multi-factor authentication on all systems in
61 accordance with this section.
62   (b) On or before July 1, 2024, the division shall Ŝ→ [adopt] **consider adopting** ←Ŝ the
62a enterprise security practices
63 described in this section and Ŝ→ [implement] **consider implementing** ←Ŝ zero trust architecture
63a and robust identity management
64 practices, including:
65   (i) multi-factor authentication;
66   (ii) cloud-based enterprise endpoint detection and response solutions to promote
67 real-time detection, and rapid investigation and remediation capabilities; and
68   (iii) robust logging practices to provide adequate data to support security investigations
69 and proactive threat hunting.
70   (4) (a) Ŝ→ [In] **If** ←Ŝ implementing a zero trust architecture and multi-factor
70a authentication, the
71 division shall Ŝ→ [prioritize] **consider prioritizing** ←Ŝ the use of third-party cloud computing
71a solutions that meet or exceed
72 industry standards.
73   (b) The division shall Ŝ→ [give] **consider giving** ←Ŝ preference to zero trust architecture
73a solutions that comply
74 with, are authorized by, or align to applicable federal guidelines, programs, and frameworks,
75 including:
76   (i) the Federal Risk and Authorization Management Program;
77   (ii) the Continuous Diagnostics and Mitigation Program; and
78   (iii) guidance and frameworks from the National Institute of Standards and
79 Technology.
80   (5) (a) In procuring third-party cloud computing solutions, the division may utilize
81 established purchasing vehicles, including cooperative purchasing contracts and federal supply
82 contracts, to facilitate efficient purchasing.
83   (b) The chief information officer shall establish a list of approved vendors that are
84 authorized to provide zero trust architecture to governmental entities in the state.
85   (c) If an executive branch agency determines that procurement of a third-party cloud
86 computing solution is not feasible, the executive branch agency shall provide a written
87 explanation to the division of the reasons that a cloud computing solution is not feasible,
88 including:
89   (i) the reasons why the executive branch agency determined that a third-party cloud

90   computing solution is not feasible;

91   (ii) specific challenges or difficulties of migrating existing solutions to a cloud

92   environment; and

93   (iii) the total expected cost of ownership of existing or alternative solutions compared

94   to a cloud computing solution.

95   (6) (a) On or before November 30 of each year, the chief information officer shall

96   report on the progress of implementing zero trust architecture and multi-factor authentication

97   to:

98   (i) the Ŝ→ [Government Operations] **Public Utilities, Energy, and Technology** ←Ŝ

98a   Interim Committee; and

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

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

101   (i) applicable guidance issued by the United States Cybersecurity and Infrastructure

102   Security Agency; and

103   (ii) the progress of the division, executive branch agencies, and governmental entities

104   with respect to:

105   (A) shifting away from a paradigm of trusted networks toward implementation of

106   security controls based on a presumption of compromise;

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

108   programs;

109   (C) limiting the ability of entities that cause incidents to move laterally through or

110   between agency systems;

111   (D) identifying incidents quickly; and

112   (E) isolating and removing unauthorized entities from agency systems as quickly as

113   practicable, accounting for cyber threat intelligence or law enforcement purposes.