

Walt Brooks proposes the following substitute bill:

Critical Infrastructure Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Walt Brooks

Senate Sponsor: Keven J. Stratton

LONG TITLE

General Description:

This bill enacts provisions regarding foreign adversary threats to state critical infrastructure.

Highlighted Provisions:

This bill:

- defines terms;
- directs the Utah Cyber Center to develop guidance on foreign adversary threats to critical infrastructure;
- authorizes voluntary security assessments for critical infrastructure involving foreign adversary technology; and
- provides for coordination between the Utah Cyber Center and state agencies on critical infrastructure security.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

ENACTS:

63A-16-1301, Utah Code Annotated 1953

63A-16-1302, Utah Code Annotated 1953

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

Section 1. Section **63A-16-1301** is enacted to read:

Part 13. Critical Infrastructure Cyber Security

63A-16-1301 . Definitions.

As used in this part:

- 29 (1) "Critical infrastructure" means systems and assets operated or maintained by a state
30 agency that are vital to the state such that the incapacity or destruction of the systems
31 and assets would have a debilitating impact on state security, state economic security, or
32 state public health, including:
33 (a) emergency services communications systems;
34 (b) electrical power systems;
35 (c) water and wastewater systems;
36 (d) transportation management systems;
37 (e) state data centers and networks; and
38 (f) systems that store or process sensitive state data or classified information.
39 (2) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.
40 (3) "Foreign adversary" means a country listed in 15 C.F.R. Sec. 791.4 as that regulation
41 existed on January 1, 2026.
42 (4) "State agency" means the same as that term is defined in Section 63A-1-103.

43 Section 2. Section **63A-16-1302** is enacted to read:

44 **63A-16-1302 . Foreign adversary threats to critical infrastructure -- Guidance**
45 **and assessments.**

- 46 (1) The Cyber Center shall, within available resources and in coordination with federal
47 agencies, develop and maintain guidance for state agencies on protecting critical
48 infrastructure from foreign adversary cybersecurity threats.
49 (2) The guidance described in Subsection (1) shall include:
50 (a) best practices for identifying and assessing security risks when foreign adversary
51 technology, software, or services are used in connection with critical infrastructure;
52 (b) recommended security controls and monitoring procedures for critical infrastructure
53 that utilizes foreign adversary technology;
54 (c) procedures for limiting foreign adversary access to critical infrastructure systems and
55 data;
56 (d) methods for assessing and documenting risks associated with foreign adversary
57 involvement in critical infrastructure;
58 (e) recommendations for transitioning away from foreign adversary technology in
59 critical infrastructure when feasible and cost-effective; and
60 (f) identification of categories of critical infrastructure that present heightened security
61 concerns if foreign adversary technology is involved.
62 (3) The Cyber Center shall:

- 63 (a) review and update the guidance described in Subsection (1) at least annually;
64 (b) make the guidance readily accessible to state agencies through the division's website;
65 and
66 (c) include information on foreign adversary threats to critical infrastructure in briefings
67 and materials provided to state agencies on cybersecurity matters.
- 68 (4) A state agency that operates or maintains critical infrastructure may request a security
69 assessment from the Cyber Center if the state agency:
70 (a) is considering procurement of technology, software, or services from a foreign
71 adversary for use in critical infrastructure; or
72 (b) identifies that critical infrastructure currently utilizes technology, software, or
73 services from a foreign adversary.
- 74 (5) The Cyber Center shall prioritize security assessment requests under Subsection (4)
75 based on:
76 (a) the sensitivity of the data or systems involved;
77 (b) the potential impact of a compromise on state security, economic security, or public
78 health;
79 (c) available Cyber Center resources; and
80 (d) other relevant factors determined by the Cyber Center.
- 81 (6) A security assessment conducted under Subsection (4) may include:
82 (a) an evaluation of potential security vulnerabilities associated with the foreign
83 adversary technology, software, or services;
84 (b) an assessment of potential risks to critical infrastructure systems and data;
85 (c) an analysis of the potential impact of a compromise of the critical infrastructure on
86 state operations, public safety, or economic security;
87 (d) recommendations for security measures or contract provisions to mitigate identified
88 risks; and
89 (e) identification of alternative technology, software, or services that may present lower
90 security risks.
- 91 (7) In conducting a security assessment under Subsection (4), the Cyber Center may:
92 (a) coordinate with the Department of Public Safety and other relevant state agencies;
93 and
94 (b) coordinate with and utilize resources from federal agencies, including the
95 Cybersecurity and Infrastructure Security Agency, as available.
- 96 (8) If the Cyber Center identifies significant security risks associated with foreign adversary

- 97 technology in critical infrastructure, the Cyber Center may:
- 98 (a) notify the chief information officer and the affected state agency of the identified
- 99 risks;
- 100 (b) recommend that the state agency implement enhanced security monitoring or
- 101 controls;
- 102 (c) recommend that the state agency develop a plan to transition to alternative
- 103 technology; or
- 104 (d) recommend that the matter be referred to appropriate state or federal law
- 105 enforcement or security agencies.
- 106 (9) A state agency that operates or maintains critical infrastructure shall, when reporting a
- 107 data breach to the Cyber Center under Section 63A-19-405, indicate whether the data
- 108 breach involved technology, software, or services from a foreign adversary.
- 109 (10) A security assessment or recommendation provided under this section is advisory only
- 110 and does not:
- 111 (a) prohibit a state agency from entering into a contract or making a procurement
- 112 decision; or
- 113 (b) require a state agency to transition away from existing technology, software, or
- 114 services.
- 115 (11) Information obtained by the Cyber Center in conducting a security assessment under
- 116 this section is protected in accordance with Title 63G, Chapter 2, Government Records
- 117 Access and Management Act.
- 118 **Section 3. Effective Date.**
- 119 This bill takes effect on May 6, 2026.