

HB016501

inserted text shows text that was not in HB0165S01 but was inserted into HB0165S02

1

Critical Infrastructure Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Walt Brooks

Senate Sponsor:

Money Appropriated in this Bill:

HB0165S01 compared with HB0165S02

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 **1** is enacted to read:

63A-16-1301. Definitions.

13. Critical Infrastructure Cyber Security

As used in this part:

(1) "Critical infrastructure" means systems and assets operated or maintained by a state agency that are vital to the state such that the incapacity or destruction of the systems and assets would have a debilitating impact on state security, state economic security, or state public health, including:

(a) emergency services communications systems;

(b) electrical power systems;

(c) water and wastewater systems;

(d) transportation management systems;

(e) state data centers and networks; and

(f) systems that store or process sensitive state data or classified information.

(2) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.

(3) "Foreign adversary" means a country listed in 15 C.F.R. Sec. 791.4 as that regulation existed on January 1, 2026.

(4) "State agency" means the same as that term is defined in Section 63A-1-103.

Section 2. Section **2** is enacted to read:

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

HB0165S01 compared with HB0165S02

- (1) The Cyber Center shall, within available resources and in coordination with federal agencies, develop and maintain guidance for state agencies on protecting critical 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 technology, software, or services are used in connection with critical infrastructure;
- 52 (b) recommended security controls and monitoring procedures for critical infrastructure that utilizes foreign adversary technology;
- 54 (c) procedures for limiting foreign adversary access to critical infrastructure systems and data;
- 56 (d) methods for assessing and documenting risks associated with foreign adversary involvement in critical infrastructure;
- 58 (e) recommendations for transitioning away from foreign adversary technology in critical infrastructure when feasible and cost-effective; and
- 60 (f) identification of categories of critical infrastructure that present heightened security 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; and
- 66 (c) include information on foreign adversary threats to critical infrastructure in briefings and materials provided to state agencies on cybersecurity matters.
- 68 (4) A state agency that operates or maintains critical infrastructure may request a security assessment from the Cyber Center if the state agency:
- 70 (a) is considering procurement of technology, software, or services from a foreign adversary for use in critical infrastructure; or
- 72 (b) identifies that critical infrastructure currently utilizes technology, software, or services from a foreign adversary.
- 74 (5) The Cyber Center shall prioritize security assessment requests under Subsection (4) 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 health;
- 79 (c) available Cyber Center resources; and
- 80 (d) other relevant factors determined by the Cyber Center.

HB0165S01 compared with HB0165S02

- (6) A security assessment conducted under Subsection (4) may include:
- (a) an evaluation of potential security vulnerabilities associated with the foreign adversary technology, software, or services;
 - (b) an assessment of potential risks to critical infrastructure systems and data;
 - (c) an analysis of the potential impact of a compromise of the critical infrastructure on state operations, public safety, or economic security;
 - (d) recommendations for security measures or contract provisions to mitigate identified risks; and
 - (e) identification of alternative technology, software, or services that may present lower security risks.
- (7) In conducting a security assessment under Subsection (4), the Cyber Center may:
- (a) coordinate with the Department of Public Safety and other relevant state agencies; and
 - (b) coordinate with and utilize resources from federal agencies, including the Cybersecurity and Infrastructure Security Agency, as available.
- (8) If the Cyber Center identifies significant security risks associated with foreign adversary technology in critical infrastructure, the Cyber Center may:
- (a) notify the chief information officer and the affected state agency of the identified risks;
 - (b) recommend that the state agency implement enhanced security monitoring or controls;
 - (c) recommend that the state agency develop a plan to transition to alternative technology; or
 - (d) recommend that the matter be referred to appropriate state or federal law enforcement or security agencies.
- (9) A state agency that operates or maintains critical infrastructure:
- (a) may not procure for use in critical infrastructure, or enter into or renew a contract or agreement for, any equipment or services identified on the covered list for federally banned equipment developed under 47 C.F.R. Sec. 1.50002; and
- (9){ (b) } { ~~A state agency that operates or maintains critical infrastructure~~ } shall, when reporting a data breach to the Cyber Center under Section 63A-19-405, indicate whether the data breach involved technology, software, or services from a foreign adversary.
- (10) { ~~A~~ } Except as provided in Subsection (9), a security assessment or recommendation provided under this section is advisory only and does not:
- (a) prohibit a state agency from entering into a contract or making a procurement decision; or
 - (b) require a state agency to transition away from existing technology, software, or services.

HB0165S01 compared with HB0165S02

(11) Information obtained by the Cyber Center in conducting a security assessment under this section is protected in accordance with Title 63G, Chapter 2, Government Records Access and Management Act.

125

Section 3. **Effective date.**

Effective Date.

This bill takes effect on May 6, 2026.

2-5-26 8:40 AM