Keven J. Stratton 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 critical infrastructure.

Highlighted Provisions:

This bill:

- defines terms;
- directs the Utah Cyber Center to develop guidance on foreign adversary threats to critical infrastructure;
- prohibits use of federally banned equipment in critical infrastructure;
- authorizes voluntary security assessments for critical infrastructure involving foreign adversary technology; and
- provides for coordination between the Utah Cyber Center and governmental entities 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:

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

(a) emergency services communications systems;

(b) electrical power systems;

(c) water and wastewater systems;

(d) transportation management systems;

(e) data centers and networks; and

(f) systems that store or process sensitive 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) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

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

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

(1) The Cyber Center shall, within available resources and in coordination with federal agencies, develop and maintain guidance for governmental entities on protecting critical infrastructure from foreign adversary cybersecurity threats.

(2) The guidance described in Subsection (1) shall include:

(a) best practices for identifying and assessing security risks when foreign adversary technology, software, or services are used in connection with critical infrastructure;

(b) recommended security controls and monitoring procedures for critical infrastructure that utilizes foreign adversary technology;

(c) procedures for limiting foreign adversary access to critical infrastructure systems and data;

(d) methods for assessing and documenting risks associated with foreign adversary involvement in critical infrastructure;

(e) recommendations for transitioning away from foreign adversary technology in critical infrastructure when feasible and cost effective;

(f) identification of categories of critical infrastructure that present heightened security concerns if foreign adversary technology is involved; and

(g) recommendations for a comprehensive manual operations contingency plan for critical infrastructure that:

(i) details non-networked, non-automated, and manually executable procedures; and

(ii) is sufficient to sustain core operational functions of the critical infrastructure in the event of a significant cyber incident that renders automated or networked control systems unreliable or inoperable.

(3) The Cyber Center shall:

(a) review and update the guidance described in Subsection (1) at least annually;

(b) make the guidance readily accessible to governmental entities through the division's website; and

(c) include information on foreign adversary threats to critical infrastructure in briefings and materials provided to governmental entities on cybersecurity matters.

(4) A governmental entity that operates or maintains critical infrastructure may request a security assessment from the Cyber Center if the governmental entity:

(a) is considering procurement of technology, software, or services from a foreign adversary for use in critical infrastructure; or

(b) identifies that critical infrastructure currently utilizes technology, software, or services from a foreign adversary.

(5) The Cyber Center shall prioritize security assessment requests under Subsection (4) based on:

(a) the sensitivity of the data or systems involved;

(b) the potential impact of a compromise on security, economic security, or public health;

(c) available Cyber Center resources; and

(d) other relevant factors determined by the Cyber Center.

(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 the governmental entity's 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 governmental entities; 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 governmental entity of the identified risks;

(b) recommend that the governmental entity implement enhanced security monitoring or controls;

(c) recommend that the governmental entity 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 governmental entity 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 security assessment or recommendation provided under this section is advisory only and does not:

(a) prohibit a governmental entity from entering into a contract or making a procurement decision; or

(b) require a governmental entity to transition away from existing technology, software, or services.

(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.

Section 3. **Effective Date.**

This bill takes effect on May 6, 2026.