HB0165S04 compared with HB0165

~~{Omitted text}~~ shows text that was in HB0165 but was omitted in HB0165S04
inserted text shows text that was not in HB0165 but was inserted into HB0165S04

DISCLAIMER: This document is provided to assist you in your comparison of the two bills. Sometimes this automated comparison will NOT be completely accurate. Therefore, you need to read the actual bills. This automatically generated document could contain inaccuracies caused by: limitations of the compare program; bad input data; or other causes.

Critical Infrastructure Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Walt Brooks

Senate Sponsor:Keven J. Stratton

LONG TITLE

General Description:

This bill {~~relates~~ } enacts provisions regarding foreign adversary threats to critical infrastructure {~~protection and communications security~~} .

Highlighted Provisions:

This bill:

- **defines terms;**
- {~~establishes requirements for access~~ } directs the Utah Cyber Center to develop guidance on foreign adversary threats to critical infrastructure {~~by foreign entities~~} ;
- {~~**requires security screening and certification for critical infrastructure access;**~~}
- prohibits {~~certain foreign adversary~~ } use of federally banned equipment in critical infrastructure;
- {~~**restricts transportation technologies and communications equipment from foreign adversaries;**~~}
- {~~**creates oversight and enforcement mechanisms;**~~}
- {~~**grants rulemaking authority to the Division of Technology Services;**~~}
-

HB0165

authorizes voluntary security assessments for critical infrastructure involving foreign adversary technology;

- provides {~~administrative penalties~~ } for {~~violations~~} coordination between the Utah Cyber Center and governmental entities on critical infrastructure security;
- {**~~establishes transition provisions for existing contracts; and~~**}
- {**~~makes technical and conforming changes.~~**}
- **prohibits governmental entities and critical infrastructure providers from contracting for or deploying technology included on a prohibited list maintained by the Utah Cyber Center;**
- **requires the Utah Cyber Center to publish and maintain a prohibited list of foreign adversary technologies that pose a risk to critical infrastructure;**
- **prohibits entities with access to critical infrastructure from entering into agreements with foreign principals that would allow remote access to or control of critical infrastructure; and**
- **authorizes the Utah Cyber Center to approve exceptions to the prohibitions under specified circumstances.**

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

63A-16-1303 , Utah Code Annotated 1953

~~{63A-16-1304 , Utah Code Annotated 1953}~~

~~{63A-16-1305 , Utah Code Annotated 1953}~~

~~{63A-16-1306 , Utah Code Annotated 1953}~~

~~{63A-16-1307 , Utah Code Annotated 1953}~~

~~{63A-16-1308 , Utah Code Annotated 1953}~~

~~{63A-16-1309 , Utah Code Annotated 1953}~~

~~{63A-16-1310 , Utah Code Annotated 1953}~~

~~{63A-16-1311 , 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.

{~~(1) {"Communications provider" means a corporation, public or private, that operates a system that supports the transmission of information of a user's choosing, regardless of the transmission medium or technology employed, that connects to a network that permits the end user to engage in communications, including service provided directly:}~~ }

{~~(a) {to the public; or}~~ }

{~~(b) {to classes of users as to be effectively available directly to the public.}~~ }

{~~(2) {"Company" means:}~~ }

{~~(a) {a for-profit sole proprietorship, organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, or limited liability company, including a wholly owned subsidiary, majority-owned subsidiary, parent company, or affiliate; or}~~ }

{~~(b) {a nonprofit organization.}~~ }

{~~(3)~~ }

13. Critical Infrastructure Cyber Security

As used in this part:

(a){(1)} "Critical infrastructure" means systems and assets {~~designated~~ } operated or maintained by {~~the division as~~ } a governmental entity that are vital to {~~this state, considering whether~~ } the governmental entity's jurisdiction such that the incapacity or destruction of the systems and assets would have a debilitating impact onsecurity, economic security, or public health, including:

{~~(i) {state security;}~~ }

{~~(ii) {state economic security; or}~~ }

{~~(iii) {state public health.}~~ }

{~~(b) {"Critical infrastructure" includes:}~~ }

(i){(a)} {~~gas and oil production, storage, or delivery~~ } emergency services communications systems;

{~~(ii) {water supply, refinement, storage, or delivery systems;}~~ }

{~~(iii) {telecommunications networks;}~~ }

(iv){(b)} electrical power {~~delivery~~ } systems;

{~~(v) {emergency services;}~~ }

(c) water and wastewater systems;

(vi){(d)} transportation management systems {~~and services; and~~} ;

(e) data centers and networks; and

(vii){(f)} {~~personal~~} systems that store or process sensitive data or classified information {~~storage systems, including cybersecurity systems~~} .

{~~(4) {"Federally banned corporation" means a company or designated equipment currently banned or at any point banned by the Federal Communications Commission, including equipment or service deemed to pose a threat to national security and identified on the covered list developed pursuant to 47 C.F.R. 1.50002 and published by the Public Safety and Homeland Security Bureau of the Federal Communications Commission pursuant to the federal Secure and Trust Communications Networks Act of 2019, 47 U.S.C. 1601 et seq.}~~ }

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

(5){(3)} "Foreign adversary" means a country listed in 15 C.F.R. Sec. 791.4 as {~~it~~} that regulation existed on January 1, {~~2025~~} 2026.

(6){(4)} "Foreign principal" means:

(a) the government or an official of the government of a foreign adversary;

(b) a political party or member of a political party or subdivision of a political party of a foreign adversary;

(c) an entity, including a partnership, association, corporation, organization, or other combination of persons organized under the laws of or having {~~its~~} a principal place of business in a foreign adversary, or a subsidiary of the entity;

(d) an individual who is domiciled in a foreign adversary and is not a citizen or lawful permanent resident of the United States; or

(e) an individual, entity, or collection of individuals or entities described in Subsections {~~(6)(a)~~} (4)(a) through (d) having a controlling interest in a partnership, association, corporation, organization, trust, or other legal entity or subsidiary formed for the purpose of owning real property.

{~~(7) {"Infrastructure technology" means:}~~ }

{~~(a) {any camera system used for enforcing traffic, including:}~~ }

{~~(i) {a speed detection system;}~~ }

{~~(ii) {a traffic infraction detector; or}~~ }

{~~(iii) {a school bus infraction detection system;}~~ }

{~~(b) {Light Detection and Ranging technology;}~~ }

{~~(c) {a Wi-Fi router; or}~~ }

{~~(d) {a modem system.}~~ }

(5) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

(6) "Information and communications technology" means any technology, system, device, application, or service used to create, collect, store, process, transmit, receive, display, or exchange information by electronic or digital means, including computers, software, networks, telecommunications systems, and related infrastructure.

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

63A-16-1302. {~~Rulemaking authority~~} Foreign adversary threats to critical infrastructure -- Guidance and assessments.

{~~The division may make rules, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, establishing:~~}

(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;

(1){(c)} procedures {~~and qualifications~~ } for {~~designating~~ } limiting foreign adversary access to critical infrastructure {~~under Section 63A-16-1301~~} 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:

(2){(a)} {~~the certification form~~ } review and {~~process~~ } update the guidance described in {~~Section 63A-16-1304~~} Subsection (1) at least annually;

{~~(3) {procedures for preapproval of contracts with foreign principals under Subsection 63A-16-1303(3);}~~ }

{~~(4) {procedures for notification and investigation of proposed sales, transfers, or investments under Section 63A-16-1305;}~~ }

(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:

(5){(a)} {~~criteria and procedures~~ } is considering procurement of technology, software, or services from a foreign adversary for {~~notifying~~ } use in critical infrastructure {~~entities of cyber threats under Subsection 63A-16-1305(5)~~} ; {~~and~~} 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) Except as provided in Subsection (12), 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.

(12) On or after July 1, 2026, a governmental entity or critical infrastructure provider may not:

(a) enter into or renew a contract with a vendor for information and communications technology that the Cyber Center has included on the prohibited list described in Subsection (13); or

(6){(b)} {~~the registration form~~ } otherwise place into service any additional information and {~~process for~~ } communications {~~providers under Section 63A-16-1309~~} technology that the Cyber Center has included on the prohibited list described in Subsection (13).

(13)

(a) On or after July 1, 2026, the Cyber Center shall publish and maintain a list of prohibited companies and information and communications technologies that the Cyber Center has assessed pose a risk of providing a foreign adversary with remote access to or control of critical infrastructure.

(b) The prohibited list shall include, at a minimum, companies and technologies that:

(i) appear on the Pentagon 1260H list;

(ii) appear on the Federal Communications Commission Covered List; or

(iii) are a re-labeled version of, or are produced by a subsidiary of a company included ina technology described in Subsection (13)(b)(i) or (ii), and for which the Cyber Center has identified that a reasonable alternative provider exists.

(14) Notwithstanding Subsection (12), a governmental entity or critical infrastructure provider may use a technology included on the prohibited list described in Subsection (13) if no reasonable alternative exists to address the need relevant to state critical infrastructure.

Section 3. Section **3** is enacted to read:

63A-16-1303. {~~Restrictions on contracting with a foreign principal for access to~~ } Foreign adversary prohibition in critical infrastructure.

(1) A company , governmental entity, or other entity {~~constructing, repairing, operating~~} that constructs, repairs, maintains, or operates critical infrastructure, or that otherwise {~~having~~ } has significant access to critical infrastructure , may not enter into {~~an~~ } a contract or other agreement relating to critical infrastructure in this state with a foreign principal from a foreign adversary if the agreement would allow the foreign principal to directly or remotely access or control critical infrastructure in this state.

{~~(2) {A governmental entity may not enter into a contract or other agreement relating to critical infrastructure in this state with a company that is a foreign principal if the agreement would allow the foreign principal to directly or remotely access or control critical infrastructure in this state.}~~ }

(3){(2)} Notwithstanding {~~Subsections~~ } Subsection (1) {~~and (2)~~} , {~~an~~ } a company, governmental entity {~~or governmental~~ } , or other entity may enter into a contract {~~relating to critical infrastructure~~ } described in Subsection (1) with a foreign principal {~~or use products or services produced by~~ } from a foreign {~~principal~~ } adversary if{~~:~~} no reasonable alternative exists to address the need relevant to state critical infrastructure.

{~~(a)~~ {~~there is no other reasonable option for addressing the need relevant to state critical infrastructure;~~} }

{~~(b)~~ {~~the contract is preapproved by the division; and~~} }

{~~(c)~~ {~~not entering into the contract would pose a greater threat to the state than the threat associated with entering into the contract.~~} }

Section 4. Section **4** is enacted to read:

63A-16-1304. Access requirements and certification.

(1) To access critical infrastructure, a company shall:

(a) file a certification form with the division; and

(b) pay a certification fee to the division.

(2) The division shall prescribe the certification form required under Subsection (1)(a).

(3) To maintain certification as a company with access to critical infrastructure, a company shall:

(a) identify all employee positions in the organization that have access to critical infrastructure;

(b) before hiring an individual described in Subsection (3)(a) or allowing the individual to continue to have access to critical infrastructure, obtain from the Department of Public Safety or a private vendor:

(i) criminal history record information relating to the prospective employee; and

(ii) other background information considered necessary by the company or required by the division to protect critical infrastructure from foreign adversary infiltration or interference;

(c) prohibit foreign nationals from a foreign adversary from access to critical infrastructure;

(d) disclose any ownership of, partnership with, or control from any entity not domiciled within the United States;

(e) store and process all data generated by critical infrastructure on domestic servers;

(f) not use cloud service providers or data centers that are foreign entities;

(g) immediately report any cyberattack, security breach, or suspicious activity to the division; and

(h) comply with Section 63A-16-1303.

(4) The division shall set the fee described in Subsection (1)(b) in an amount sufficient to cover the costs of administering the certification process but not to exceed $150.

(5) The division shall:

(a) determine whether a company is compliant with all requirements of this section; or

(b) revoke certification.

Section 5. Section **5** is enacted to read:

63A-16-1305. Division powers and duties.

(1) An owner of a critical infrastructure installation shall notify the division of any proposed sale or transfer of, or investment in, the critical infrastructure to:

(a) an entity domiciled outside of the United States; or

(b) an entity with any foreign adversary ownership.

(2) The division shall have no more than 30 days following the notice described in Subsection (1) to investigate the proposed sale, transfer, or investment.

(3) The attorney general, on behalf of the division, may file an action in district court requesting an injunction opposing the proposed sale, transfer, or investment, if the division determines that a proposed sale, transfer, or investment described in Subsection (1) threatens:

(a) state critical infrastructure security;

(b) state economic security; or

(c) state public health.

(4) If a district court finds, in an action brought under Subsection (3), that a challenged sale, transfer, or investment in critical infrastructure poses a reasonable threat to critical infrastructure security, economic security, or public health, the district court may issue an order enjoining the challenged sale, transfer, or investment.

(5) The division shall notify critical infrastructure entities of known or suspected cyber threats, vulnerabilities, and adversarial activities in a manner consistent with the goals of:

(a) identifying and closing similar exploits in similar critical infrastructure installations or processes;

(b) maintaining operational security and normal functioning of critical infrastructure; and

(c) protecting the rights of private critical infrastructure entities, including by reducing the extent to which trade secrets or other proprietary information is shared between entities, to the extent that the precaution does not inhibit the ability of the division to effectively communicate the threat of a known or suspected exploit or adversarial activity.

Section 6. Section **6** is enacted to read:

63A-16-1306. Prohibited software and equipment.

(1) Software used in state infrastructure located within or serving this state may not include any software produced by a company headquartered in and subject to the laws of a foreign adversary, or a company under the direction or control of a foreign adversary.

(2) Software used in state infrastructure in operation within or serving this state, including any state infrastructure that is not permanently disabled, shall have all software prohibited by Subsection (1) removed and replaced with software that is not prohibited by Subsection (1).

(3) A state infrastructure provider that removes, discontinues, or replaces any prohibited software is not required to obtain any additional permits from any state agency or political subdivision for the removal, discontinuance, or replacement of the software if:

(a) the state agency or political subdivision is properly notified of the necessary replacements; and

(b) the replacement software is similar to the existing software.

Section 7. Section **7** is enacted to read:

63A-16-1307. Infrastructure technology restrictions.

(1) On or after July 1, 2025, a governmental entity may not knowingly enter into or renew a contract with a contracting vendor of prohibited infrastructure technology if:

(a) the contracting vendor is owned by the government of a foreign adversary;

(b) the government of a foreign adversary has a controlling interest in the contracting vendor; or

(c) the contracting vendor is selling a product produced by:

(i) a government of a foreign adversary;

(ii) a company primarily domiciled in a foreign adversary; or

(iii) a company owned or controlled by a company primarily domiciled in a foreign adversary.

(2) On or after July 1, 2025, each critical infrastructure provider in this state shall certify to the division that it does not use any Wi-Fi router or modem system described in Subsections (1)(a) through (c).

(3) On or after July 1, 2025, the division shall create, maintain, and update a public listing of prohibited infrastructure technology for government entities and critical infrastructure providers.

Section 8. Section **8** is enacted to read:

63A-16-1308. Communications equipment prohibitions.

(1) Critical communications infrastructure located within or serving this state shall be constructed not to include any equipment manufactured by a federally banned corporation.

(2) Critical communications infrastructure in operation within or serving this state, including any critical communications infrastructure that is not permanently disabled, shall have all equipment prohibited by this section removed and replaced with equipment that is not prohibited by this section.

(3) A communications provider that removes, discontinues, or replaces any prohibited communications equipment or service is not required to obtain any additional permits from any state agency or political subdivision for the removal, discontinuance, or replacement of the communications equipment or service if:

(a) the state agency or political subdivision is properly notified of the necessary replacements; and

(b) the replacement communications equipment is similar to the existing communications equipment.

Section 9. Section **9** is enacted to read:

63A-16-1309. Communications provider registration.

(1) A communications provider providing service in this state that utilizes equipment from a federally banned corporation in providing service to this state shall:

(a) file a registration form with the division by September 1, 2025;

(b) pay a registration fee to the division; and

(c) file a registration form with the division on January 1 of each year.

(2) A communications provider shall register with the division before providing service.

(3) The division shall prescribe the registration form required under this section.

(4) A communications provider shall provide the division with the name, address, telephone number, and email address of an individual with managerial responsibility for the Utah operations.

(5) A communications provider shall:

(a) submit a registration fee at the time of submission of the registration form;

(b) keep the information required by this section current and notify the division of any changes to the information within 60 days after the change; and

(c) certify to the division by January 1 of each year all instances of prohibited critical communications equipment or services described in Section 63A-16-1308 if the communications provider is a participant in the Federal Secure and Trusted Communications Networks Reimbursement Program, established by the federal Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. Sec. 1601 et seq., along with the geographic coordinates of the areas served by the prohibited equipment.

(6) If a communications provider certifies to the division that it is a participant in the Federal Secure and Trusted Communications Networks Reimbursement Program in accordance with, Subsection (5)(c), the communications provider shall submit a status report to the division every quarter that details the communications provider's compliance with the reimbursement program.

(7) The division shall set the registration fee described in Subsection (5)(a) in an amount sufficient to cover the costs of administering the registration process but not to exceed $50.

Section 10. Section **10** is enacted to read:

63A-16-1310. Administrative penalties and enforcement.

(1) The division may, in accordance with Title 63G, Chapter 4, Administrative Procedures Act, impose an administrative fine on a communications provider that violates Section 63A-16-1309 of not less than $5,000 per day and not more than $25,000 per day of noncompliance.

(2) The division may, in accordance with Title 63G, Chapter 4, Administrative Procedures Act, impose an administrative fine on a communications provider that knowingly submits a false registration form described in Section 63A-16-1309 of not less than $10,000 per day and not more than $20,000 per day of noncompliance.

(3) A communications provider that fails to comply with Section 63A-16-1309 is prohibited from receiving:

(a) state or local funds for the development or support of new or existing critical communications infrastructure, including the Utah Communications Universal Service Fund; and

(b) federal funds subject to distribution by state or local governments for the development or support of new or existing critical communications infrastructure.

(4) The division shall develop and publish, on a quarterly basis, a map of known prohibited communications equipment described in Section 63A-16-1308 within all communications within or serving this state.

(5) The map described in Subsection (4) shall:

(a) clearly show the location of the prohibited equipment and the communications area serviced by the prohibited equipment;

(b) state the communications provider responsible for the prohibited equipment;

(c) make clearly legible the areas serviced by the prohibited equipment; and

(d) describe the nature of the prohibited equipment by stating, at minimum, the prohibited equipment manufacturer and equipment type or purpose.

Section 11. Section **11** is enacted to read:

63A-16-1311. Transition provisions.

(1)

(a) A contract or agreement in effect on the effective date of this part that would be prohibited under this part may continue in effect until 12 months after the effective date of this part.

(b) A contract or agreement described in Subsection (1)(a) may not be renewed, extended, or modified to extend the term beyond the date described in Subsection (1)(a).

(2)

(a) A governmental entity or critical infrastructure provider that entered into a contract or agreement described in Subsection (1) shall notify the division of the contract or agreement within 60 days after the effective date of this part.

(b) The notification described in Subsection (2)(a) shall include:

(i) the nature of the contract or agreement;

(ii) the foreign principal or foreign adversary involved;

(iii) the critical infrastructure, equipment, or services covered by the contract or agreement;

(iv) the expected termination date of the contract or agreement; and

(v) any security measures currently in place to mitigate risks.

(3) The division may, after consultation with the Department of Public Safety, require additional security measures for contracts or agreements continuing under Subsection (1) if the division determines that the contract or agreement poses an unacceptable risk to state security.

(4)

(a) A communications provider that utilizes equipment from a federally banned corporation on the effective date of this part shall:

(i) register with the division within 90 days after the effective date of this part; and

(ii) submit a plan for removing and replacing the prohibited equipment within 12 months after the effective date of this part.

(b) A communications provider that fails to submit a plan described in Subsection (4)(a)(ii) within the required timeframe is prohibited from receiving state or federal funds as described in Subsection 63A-16-1310(3).

(5) Critical infrastructure providers using prohibited transportation technology on the effective date of this part shall certify compliance with Section 63A-16-1307 within 12 months after the effective date of this part.

(6) This section applies to contracts and agreements relating to:

(a) critical infrastructure under Section 63A-16-1303;

(b) prohibited software and equipment under Section 63A-16-1306;

(c) prohibited infrastructure technology under Section 63A-16-1307;

(d) communications equipment under Section 63A-16-1308; and

(e) communications provider registration under Section 63A-16-1309.

Section 4. **Effective date.**

Effective Date.

This bill takes effect on May 6, 2026.

2-27-26 2:02 PM