

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

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;
 - ▶ provides for coordination between the Utah Cyber Center and governmental entities on critical infrastructure security;
 - ▶ 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

28 **Other Special Clauses:**

29 None

30 **Utah Code Sections Affected:**

31 ENACTS:

32 **63A-16-1301**, Utah Code Annotated 195333 **63A-16-1302**, Utah Code Annotated 195334 **63A-16-1303**, Utah Code Annotated 1953

35

36 *Be it enacted by the Legislature of the state of Utah:*37 Section 1. Section **63A-16-1301** is enacted to read:38 **Part 13. Critical Infrastructure Cyber Security**39 **63A-16-1301 . Definitions.**40 As used in this part:

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

45 (a) emergency services communications systems;46 (b) electrical power systems;47 (c) water and wastewater systems;48 (d) transportation management systems;49 (e) data centers and networks; and50 (f) systems that store or process sensitive data or classified information.51 (2) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.

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

54 (4) "Foreign principal" means:55 (a) the government or an official of the government of a foreign adversary;

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

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

61 (d) an individual who is domiciled in a foreign adversary and is not a citizen or lawful

- 62 permanent resident of the United States; or
- 63 (e) an individual, entity, or collection of individuals or entities described in Subsections
- 64 (4)(a) through (d) having a controlling interest in a partnership, association,
- 65 corporation, organization, trust, or other legal entity or subsidiary formed for the
- 66 purpose of owning real property.
- 67 (5) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
- 68 (6) "Information and communications technology" means any technology, system, device,
- 69 application, or service used to create, collect, store, process, transmit, receive, display, or
- 70 exchange information by electronic or digital means, including computers, software,
- 71 networks, telecommunications systems, and related infrastructure.

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

73 **63A-16-1302 . Foreign adversary threats to critical infrastructure -- Guidance**

74 **and assessments.**

- 75 (1) The Cyber Center shall, within available resources and in coordination with federal
- 76 agencies, develop and maintain guidance for governmental entities on protecting critical
- 77 infrastructure from foreign adversary cybersecurity threats.
- 78 (2) The guidance described in Subsection (1) shall include:
- 79 (a) best practices for identifying and assessing security risks when foreign adversary
- 80 technology, software, or services are used in connection with critical infrastructure;
- 81 (b) recommended security controls and monitoring procedures for critical infrastructure
- 82 that utilizes foreign adversary technology;
- 83 (c) procedures for limiting foreign adversary access to critical infrastructure systems and
- 84 data;
- 85 (d) methods for assessing and documenting risks associated with foreign adversary
- 86 involvement in critical infrastructure;
- 87 (e) recommendations for transitioning away from foreign adversary technology in
- 88 critical infrastructure when feasible and cost effective;
- 89 (f) identification of categories of critical infrastructure that present heightened security
- 90 concerns if foreign adversary technology is involved; and
- 91 (g) recommendations for a comprehensive manual operations contingency plan for
- 92 critical infrastructure that:
- 93 (i) details non-networked, non-automated, and manually executable procedures; and
- 94 (ii) is sufficient to sustain core operational functions of the critical infrastructure in
- 95 the event of a significant cyber incident that renders automated or networked

96 control systems unreliable or inoperable.

97 (3) The Cyber Center shall:

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

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

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

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

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

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

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

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

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

113 (c) available Cyber Center resources; and

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

115 (6) A security assessment conducted under Subsection (4) may include:

116 (a) an evaluation of potential security vulnerabilities associated with the foreign
117 adversary technology, software, or services;

118 (b) an assessment of potential risks to critical infrastructure systems and data;

119 (c) an analysis of the potential impact of a compromise of the critical infrastructure on
120 the governmental entity's operations, public safety, or economic security;

121 (d) recommendations for security measures or contract provisions to mitigate identified
122 risks; and

123 (e) identification of alternative technology, software, or services that may present lower
124 security risks.

125 (7) In conducting a security assessment under Subsection (4), the Cyber Center may:

126 (a) coordinate with the Department of Public Safety and other relevant governmental
127 entities; and

128 (b) coordinate with and utilize resources from federal agencies, including the
129 Cybersecurity and Infrastructure Security Agency, as available.

- 130 (8) If the Cyber Center identifies significant security risks associated with foreign adversary
131 technology in critical infrastructure, the Cyber Center may:
- 132 (a) notify the chief information officer and the affected governmental entity of the
133 identified risks;
- 134 (b) recommend that the governmental entity implement enhanced security monitoring or
135 controls;
- 136 (c) recommend that the governmental entity develop a plan to transition to alternative
137 technology; or
- 138 (d) recommend that the matter be referred to appropriate state or federal law
139 enforcement or security agencies.
- 140 (9) A governmental entity that operates or maintains critical infrastructure shall, when
141 reporting a data breach to the Cyber Center under Section 63A-19-405, indicate whether
142 the data breach involved technology, software, or services from a foreign adversary.
- 143 (10) Except as provided in Subsection (12), a security assessment or recommendation
144 provided under this section is advisory only and does not:
- 145 (a) prohibit a governmental entity from entering into a contract or making a procurement
146 decision; or
- 147 (b) require a governmental entity to transition away from existing technology, software,
148 or services.
- 149 (11) Information obtained by the Cyber Center in conducting a security assessment under
150 this section is protected in accordance with Title 63G, Chapter 2, Government Records
151 Access and Management Act.
- 152 (12) On or after July 1, 2026, a governmental entity or critical infrastructure provider may
153 not:
- 154 (a) enter into or renew a contract with a vendor for information and communications
155 technology that the Cyber Center has included on the prohibited list described in
156 Subsection (13); or
- 157 (b) otherwise place into service any additional information and communications
158 technology that the Cyber Center has included on the prohibited list described in
159 Subsection (13).
- 160 (13)(a) On or after July 1, 2026, the Cyber Center shall publish and maintain a list of
161 prohibited companies and information and communications technologies that the
162 Cyber Center has assessed pose a risk of providing a foreign adversary with remote
163 access to or control of critical infrastructure.

164 (b) The prohibited list shall include, at a minimum, companies and technologies that:
165 (i) appear on the Pentagon 1260H list;
166 (ii) appear on the Federal Communications Commission Covered List; or
167 (iii) are a re-labeled version of, or are produced by a subsidiary of a company
168 included in a technology described in Subsection (13)(b)(i) or (ii), and for which
169 the Cyber Center has identified that a reasonable alternative provider exists.

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

174 Section 3. Section **63A-16-1303** is enacted to read:

175 **63A-16-1303 . Foreign adversary prohibition in critical infrastructure.**

176 (1) A company, governmental entity, or other entity that constructs, repairs, maintains, or
177 operates critical infrastructure, or that otherwise has significant access to critical
178 infrastructure, may not enter into a contract or other agreement relating to critical
179 infrastructure in this state with a foreign principal from a foreign adversary if the
180 agreement would allow the foreign principal to directly or remotely access or control
181 critical infrastructure in this state.

182 (2) Notwithstanding Subsection (1), a company, governmental entity, or other entity may
183 enter into a contract described in Subsection (1) with a foreign principal from a foreign
184 adversary if no reasonable alternative exists to address the need relevant to state critical
185 infrastructure.

186 Section 4. **Effective Date.**

187 This bill takes effect on May 6, 2026.