**South Carolina General Assembly**

126th Session, 2025-2026

**H. 4393**

**STATUS INFORMATION**

General Bill

Sponsors: Reps. Hartnett, Bradley, Erickson, Brewer, W. Newton and Teeple

Document Path: LC-0237DG25.docx

Introduced in the House on April 23, 2025

Currently residing in the House Committee on **Labor, Commerce and Industry**

Summary: South Carolina Technology Security Act

**HISTORY OF LEGISLATIVE ACTIONS**

Date Body Action Description with journal page number

4/23/2025 House Introduced and read first time ([House Journal‑page 52](h:\hj\20250423.docx))

4/23/2025 House Referred to Committee on **Labor, Commerce and Industry** ([House Journal‑page 52](h:\hj\20250423.docx))

View the latest  [legislative information](https://www.scstatehouse.gov/billsearch.php?billnumbers=4393&session=126&summary=B)  at the website

**VERSIONS OF THIS BILL**

[04/23/2025](https://www.scstatehouse.gov/sess126_2025-2026/prever/4393_20250423.docx)

A bill

TO AMEND THE SOUTH CAROLINA CODE OF LAWS BY ENACTING THE “SOUTH CAROLINA TECHNOLOGY SECURITY ACT” BY ADDING ARTICLE 29 TO CHAPTER 1, TITLE 1 SO AS TO PROHIBIT THE PURCHASE AND USE OF CERTAIN TELECOMMUNICATIONS EQUIPMENT, VIDEO SURVEILLANCE EQUIPMENT, OR HARDWARE OR SOFTWARE THAT IS MANUFACTURED OR DISTRIBUTED BY CERTAIN BANNED COMPANIES.

Whereas, the United States Department of Defense (DoD) has identified certain companies, including Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company (Hikvision), and Zhejiang Dahua Technology Company (Dahua), whose products and services may pose a risk to national security; and

Whereas, the State of South Carolina has a compelling interest in safeguarding its citizens, public agencies, and infrastructure from potential security vulnerabilities arising from the use of telecommunications and video surveillance technology; and

Whereas, it is in the interest of the State of South Carolina to prohibit the purchase, sale, or use of these products and services by public and private entities to ensure the safety and security of its people. Now, therefore,

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. This act may be cited as the “South Carolina Technology Security Act.”

SECTION 2. Chapter 1, Title 1 of the S.C. Code is amended by adding:

Article 29

Statewide Provisions

Section 1‑1‑1910. (A) As used in this section:

(1) “Banned company” means any Chinese‑owned entity, including any subsidiaries, affiliates, or successor entities thereof including, but not limited to: Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company (Hikvision), and Zhejiang Dahua Technology Company (Dahua).

(2) “Covered products or services” means, but is not limited to, telecommunications, video surveillance, or container tracking technology equipment, and any parts of such equipment that is manufactured, assembled, or distributed by a banned company.

(3) “Person” means an individual, corporation, business trust, partnership, or any other legal or commercial entity.

(4) “Political Subdivision” means all political subdivisions of this State, including school districts.

(5) “State Agency” means any state office, department, board, commission, institution, or any other division of state government.

(B)(1) No state agency or political subdivision may purchase, lease, or otherwise acquire covered products or services from a banned company.

(2) No state agency or political subdivision may use or permit the use of covered products or services in the performance of a contract, grant, or any publicly funded project.

(C)(1) No person in this State may offer for sale or sell any covered products or services from a banned company within the State of South Carolina.

(2) No person in this State shall install or use any covered products or services from a banned company in any commercial capacity including, but not limited to, telecommunications infrastructure or security surveillance applications.

(D)(1) In the event of an emergency declared by the Governor, a state agency, political subdivision, or person may acquire or use covered products or services if no other viable alternative is available, and the acquisition or use is strictly necessary for the protection of life or property. Any such acquisition or use must be immediately reported in writing to the Attorney General, with a detailed justification of the circumstances.

(2) Notwithstanding subsection (E), it shall be unlawful for any person, state agency, or political subdivision to use covered products or services that remain in place pursuant to an existing contract for the purpose of transmitting data to the People’s Republic of China, or to any country, person, or entity acting as an intermediary to facilitate such transmission.

(E) All container tracking technology, regardless of source, must be reviewed and approved by the South Coast Cyber Center or another South Carolina based nonprofit cybersecurity organization that focuses on maritime cybersecurity before the container tracking technology is put into operation.

(F)(1) The Office of the Attorney General, in coordination with any other relevant state authority, shall have the power to investigate any potential violations of this section and to bring civil or administrative actions to enforce compliance.

(2)(a) A Person who knowingly violates the provisions of this section may be subject to a civil penalty not to exceed ten thousand dollars per day for each day of noncompliance, as determined by a court of competent jurisdiction.

(b) A state agency or political subdivision found to be in violation of this section may be subject to administrative penalties not to exceed ten thousand dollars per day for each day of noncompliance.

(3) Any person, state agency, or political subdivision that knowingly and wilfully uses covered products or services to transmit data to the People’s Republic of China, or to any country, person, or entity acting as an intermediary for such transmission, in violation of subsection (D)(2), is guilty of a felony punishable by a fine of not more than fifty thousand dollars, imprisonment for not more than twenty‑five years, or both, as determined by a court of competent jurisdiction.

(G) The Attorney General shall submit an annual report to the Governor, the President of the Senate, and the Speaker of the House of Representatives by December thirty‑first of each year, summarizing:

(1) the number and nature of investigations conducted under this section;

(2) the outcome of these investigations, including penalties imposed and corrective measures taken; and

(3) recommendations, if any, for additional legislative or administrative actions to enhance the enforcement and effectiveness of this section.

SECTION 3. Any current contract between a state agency or political subdivision and any entity for the procurement or use of any covered products or services in violation of this act is null and void.

SECTION 4. If any section, subsection, paragraph, subparagraph, sentence, clause, phrase, or word of this act is for any reason held to be unconstitutional or invalid, such holding shall not affect the constitutionality or validity of the remaining portions of this act, the General Assembly hereby declaring that it would have passed this act, and each and every section, subsection, paragraph, subparagraph, sentence, clause, phrase, and word thereof, irrespective of the fact that any one or more other sections, subsections, paragraphs, subparagraphs, sentences, clauses, phrases, or words hereof may be declared to be unconstitutional, invalid, or otherwise ineffective.

SECTION 5. This act takes effect upon approval by the Governor.

‑‑‑‑XX‑‑‑‑