S. 29

116TH CONGRESS
1ST SESSION

To establish the Office of Critical Technologies and Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES
JANUARY 4, 2019

Mr. WARNER (for himself and Mr. RUBIO) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL
To establish the Office of Critical Technologies and Security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. FINDING; PURPOSE.

(a) FINDING.—Congress finds that, as of the date of the enactment of this Act, the Federal Government lacked—

(1) an office in the Executive Office of the President that can coordinate security policy relating to critical emerging, foundational, and dual-use technologies between the National Security Council and
the National Economic Council and interface with international, Federal, State, and local entities on that policy; and

(2) a strategic plan—

(A) to stop the transfer of critical emerging, foundational, and dual-use technologies to countries that pose a national security risk; and

(B) to maintain United States technological leadership with respect to critical emerging, foundational, and dual-use technologies and ensure supply chain integrity and security for such technologies.

(b) PURPOSE.—The primary purpose of this Act is to establish the Office of Critical Technologies and Security—

(1) to coordinate a whole-of-government response to protect critical emerging, foundational, and dual-use technologies and to effectively enlist the support of regulators, the private sector, and other scientific and technical hubs, including academia, to support and assist with such response; and

(2) to develop a long-term strategy to achieve and maintain United States technological supremacy with respect to critical emerging, foundational, and
dual-use technologies and ensure supply chain integrity and security for such technologies.

SEC. 2. OFFICE OF CRITICAL TECHNOLOGIES AND SECURITY.

(a) ESTABLISHMENT.—There is established in the Executive Office of the President an Office of Critical Technology and Security (in this section referred to as the “Office”).

(b) DIRECTOR.—

(1) IN GENERAL.—There shall be at the head of the Office a Director who shall be appointed by the President.

(2) REPORTING.—The Director of the Office shall report directly to the President.

(3) ADDITIONAL ROLES.—In addition to serving as the head of the Office, the Director of the Office shall—

(A) be a Deputy National Security Advisor for the National Security Council and serve as a member of such council;

(B) be a Deputy Director for the National Economic Council and serve as a member of such council; and
(C) serve as the chairperson of the Council on Critical Technologies and Security established under section 3.

(c) FUNCTIONS.—The functions of the Director of the Office are as follows:

(1) COORDINATION.—To carry out coordination functions as follows:

(A) To serve as a centralized focal point within the Executive Office of the President for coordinating policy and actions of the Federal Government—

(i) to stop the transfer of critical emerging, foundational, and dual-use technologies to countries that pose a national security risk, including by leading the interagency process to identify emerging and foundational technologies under section 1758 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232); and

(ii) to maintain United States technological leadership with respect to critical emerging, foundational, and dual-use technologies and ensure supply chain integrity and security for such technologies.
(B) To coordinate whole-of-government responses, working in partnership with heads of national security and economic agencies and agencies with science and technology hubs, including those described in section 3(c)(1).

(C) To facilitate coordination and consultation with—

(i) Federal and State regulators of telecommunications and technology industries, including the Federal Communications Commission, the Federal Trade Commission, and the Office of Science and Technology Policy;

(ii) the private sector, including industry, labor, consumer, and other groups as necessary;

(iii) other nongovernmental scientific and technical hubs and stakeholders, including academic stakeholders; and

(iv) key international partners and allies of the United States.

(2) MESSAGING AND OUTREACH.—To lead messaging and outreach efforts by the Federal Government on the national security threat posed by the improper acquisition and transfer of critical emerg-
ing, foundational, and dual-use technologies that the Federal Government determines necessary to protect, by countries of concern including—

(A) acting as the chief policy spokesperson for the Federal Government on related security and critical technology issues;

(B) encouraging Federal departments and agencies to work with key stakeholders as described in paragraph (1), as well as States, localities, international partners, and allies, to better analyze and disseminate critical information from the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)); and

(C) improving overall education of the United States public and business leaders in key sectors about the threat to United States national security posed by—

(i) the improper acquisition and transfer of critical technologies by countries that pose a national security risk; and

(ii) reliance on foreign products identified by the Federal Government that pose a national security risk in private sector supply chains.
(3) Long-term Strategy.—To lead the development of a comprehensive, long-term strategic plan in coordination with United States allies and other defense partners—

(A) to enhance the interagency process for identifying emerging and foundational carried out under section 1758 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) and to re-evaluate those identifications on an ongoing basis;

(B)(i) to protect and enforce intellectual property rights;

(ii) to reduce reliance on foreign products identified by the Federal Government that pose a national security risk to the United States in critical public sector supply chains;

(iii) to develop a strategy to inform the private sector about critical supply chain risks;

and

(iv) to address other security concerns related to forced or unfair technology transfer to and from such countries;

(C) to maintain technological leadership with respect to critical emerging, foundational,
and dual-use technologies and to increase public sector funding for research and development that is key to maintaining such technological leadership;

(D) to develop specific policies and actions to enforce intellectual property and cybersecurity standards to deter and prosecute industrial espionage and other similar measures; and

(E) to develop specific policies—

(i) to improve the research and development ecosystem, including academic institutions, nonprofit organizations, and private entities; and

(ii) to reestablish the United States as the world leader in research and development; and

(F) to develop specific measures and goals that can be tracked and monitored as described in paragraph (4).

(4) MONITORING AND TRACKING.—

(A) MEASURES.—In conjunction with the Council of Economic Advisors, the United States Trade Representative, the Office of Science and Technology Policy, to use measures
developed under paragraph (3)(F) to monitor and track—

(i) key trends relating to transfer of critical emerging, foundational, and dual-use technologies;

(ii) key trends relating to United States government investments in innovation and competitiveness compared to governments of other countries;

(iii) inappropriate influence of international standards setting processes by foreign countries that pose a national security risk; and

(iv) progress implementing the comprehensive, long-term strategic plan developed under paragraph (3).

(B) GOALS.—To monitor and track progress made towards achieving goals relating to protecting the security of critical technologies of the United States.

(d) STAFF.—The Director of the Office may—

(1) without regard to the civil service laws, employ, and fix the compensation of, such specialists and other experts as may be necessary for the Director to carry out the functions of the Director; and
(2) subject to the civil service laws, employ such other officers and employees as may be necessary to carry out the functions of the Director.

(e) Annual Report.—

(1) In general.—Not less frequently than once each year, the Director shall submit to Congress a report on—

(A) the activities of the Office; and

(B) matters relating to national security and the protection of critical technologies.

(2) Form.—Each report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(f) Conforming Amendment.—Section 101(e) of the National Security Act of 1947 (50 U.S.C. 3021(c)) is amended by inserting “the Director of the Office of Critical Technologies and Security,” after “Treasury,”.

SEC. 3. COUNCIL ON CRITICAL TECHNOLOGIES AND SECURITY.

(a) Establishment.—There is a council known as the Council on Critical Technologies and Security (in this section referred to as the “Council”).

(b) Function.—The function of the Council shall be to advise the President on matters relating to challenges
posed by foreign powers with respect to technology acquisition and transfer.

(c) Membership.—

(1) Composition.—The Council shall be composed of the following:

(A) The Director of the Office of Critical Technologies and Security appointed under section 2(b)(1).

(B) The Secretary of Agriculture.

(C) The Secretary of Commerce.

(D) The Secretary of Defense.

(E) The Secretary of Education.

(F) The Secretary of Energy.

(G) The Secretary of Homeland Security.

(H) The Secretary of State.

(I) The Secretary of Transportation.

(J) The Secretary of the Treasury.

(K) The Director of the Office of Management and Budget.

(L) The Director of National Intelligence.

(M) The Director of the Central Intelligence Agency.

(N) The Director of the Federal Bureau of Investigation.
(O) The United States Trade Representative.

(P) The Director of the National Economic Council.

(Q) The National Security Advisor.

(R) The Director of the Office of Science and Technology Policy.

(S) A representative of the Committee on Foreign Investment in the United States who shall be selected by the Committee for purposes of this section.


(U) The Chair of the Federal Communications Commission.

(V) The Chair of the Federal Trade Commission.

(W) Such other heads of departments and agencies of the Federal Government as the chairperson of the Council considers appropriate.

(2) CHAIRPERSON.—The chairperson of the Council shall be the Director of the Office of Critical Technologies and Security appointed under section 2(b)(1).
(d) Consultation and Cooperation.—The Council—

(1) may constitute such advisory committees and may consult with such representatives of industry, agriculture, labor, consumers, State and local governments, and other groups, as the Council considers advisable;

(2) shall consult with the entities listed under section 2(c)(1)(C); and

(3) shall seek and obtain the cooperation of the various executive and independent agencies of the Federal Government in the development of specialized studies essential to its responsibilities.