

116TH CONGRESS  
1ST SESSION

# S. 29

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.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. FINDING; PURPOSE.**

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

7 (1) an office in the Executive Office of the  
8 President that can coordinate security policy relating  
9 to critical emerging, foundational, and dual-use tech-  
10 nologies between the National Security Council and

1 the National Economic Council and interface with  
2 international, Federal, State, and local entities on  
3 that policy; and

4 (2) a strategic plan—

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

8 (B) to maintain United States techno-  
9 logical leadership with respect to critical emerg-  
10 ing, foundational, and dual-use technologies and  
11 ensure supply chain integrity and security for  
12 such technologies.

13 (b) PURPOSE.—The primary purpose of this Act is  
14 to establish the Office of Critical Technologies and Secu-  
15 rity—

16 (1) to coordinate a whole-of-government re-  
17 sponse to protect critical emerging, foundational,  
18 and dual-use technologies and to effectively enlist  
19 the support of regulators, the private sector, and  
20 other scientific and technical hubs, including aca-  
21 demia, to support and assist with such response; and

22 (2) to develop a long-term strategy to achieve  
23 and maintain United States technological supremacy  
24 with respect to critical emerging, foundational, and

1 dual-use technologies and ensure supply chain integ-  
2 rity and security for such technologies.

3 **SEC. 2. OFFICE OF CRITICAL TECHNOLOGIES AND SECUR-**  
4 **RITY.**

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

9 (b) DIRECTOR.—

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

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

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

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

21 (B) be a Deputy Director for the National  
22 Economic Council and serve as a member of  
23 such council; and

1           (C) serve as the chairperson of the Council  
2           on Critical Technologies and Security estab-  
3           lished under section 3.

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

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

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

12           (i) to stop the transfer of critical  
13          emerging, foundational, and dual-use tech-  
14          nologies to countries that pose a national  
15          security risk, including by leading the  
16          interagency process to identify emerging  
17          and foundational technologies under sec-  
18          tion 1758 of the John S. McCain National  
19          Defense Authorization Act for Fiscal Year  
20          2019 (Public Law 115–232); and

21           (ii) to maintain United States techno-  
22          logical leadership with respect to critical  
23          emerging, foundational, and dual-use tech-  
24          nologies and ensure supply chain integrity  
25          and security for such technologies.

1 (B) To coordinate whole-of-government re-  
2 sponses, working in partnership with heads of  
3 national security and economic agencies and  
4 agencies with science and technology hubs, in-  
5 cluding those described in section 3(e)(1).

6 (C) To facilitate coordination and consulta-  
7 tion with—

8 (i) Federal and State regulators of  
9 telecommunications and technology indus-  
10 tries, including the Federal Communica-  
11 tions Commission, the Federal Trade Com-  
12 mission, and the Office of Science and  
13 Technology Policy;

14 (ii) the private sector, including indus-  
15 try, labor, consumer, and other groups as  
16 necessary;

17 (iii) other nongovernmental scientific  
18 and technical hubs and stakeholders, in-  
19 cluding academic stakeholders; and

20 (iv) key international partners and al-  
21 lies of the United States.

22 (2) MESSAGING AND OUTREACH.—To lead mes-  
23 saging and outreach efforts by the Federal Govern-  
24 ment on the national security threat posed by the  
25 improper acquisition and transfer of critical emerg-

1 ing, foundational, and dual-use technologies that the  
2 Federal Government determines necessary to pro-  
3 tect, by countries of concern including—

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

7 (B) encouraging Federal departments and  
8 agencies to work with key stakeholders as de-  
9 scribed in paragraph (1), as well as States, lo-  
10 calities, international partners, and allies, to  
11 better analyze and disseminate critical informa-  
12 tion from the intelligence community (as de-  
13 fined in section 3 of the National Security Act  
14 of 1947 (50 U.S.C. 3003)); and

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

19 (i) the improper acquisition and trans-  
20 fer of critical technologies by countries  
21 that pose a national security risk; and

22 (ii) reliance on foreign products iden-  
23 tified by the Federal Government that pose  
24 a national security risk in private sector  
25 supply chains.

1           (3) LONG-TERM STRATEGY.—To lead the devel-  
2           opment of a comprehensive, long-term strategic plan  
3           in coordination with United States allies and other  
4           defense partners—

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

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

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

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

21                   (iv) to address other security concerns re-  
22                   lated to forced or unfair technology transfer to  
23                   and from such countries;

24                   (C) to maintain technological leadership  
25                   with respect to critical emerging, foundational,

1 and dual-use technologies and to increase public  
2 sector funding for research and development  
3 that is key to maintaining such technological  
4 leadership;

5 (D) to develop specific policies and actions  
6 to enforce intellectual property and cybersecu-  
7 rity standards to deter and prosecute industrial  
8 espionage and other similar measures; and

9 (E) to develop specific policies—

10 (i) to improve the research and devel-  
11 opment ecosystem, including academic in-  
12 stitutions, nonprofit organizations, and pri-  
13 vate entities; and

14 (ii) to reestablish the United States as  
15 the world leader in research and develop-  
16 ment; and

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

20 (4) MONITORING AND TRACKING.—

21 (A) MEASURES.—In conjunction with the  
22 Council of Economic Advisors, the United  
23 States Trade Representative, the Office of  
24 Science and Technology Policy, to use measures



1 developed under paragraph (3)(F) to monitor  
2 and track—

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

6 (ii) key trends relating to United  
7 States government investments in innova-  
8 tion and competitiveness compared to gov-  
9 ernments of other countries;

10 (iii) inappropriate influence of inter-  
11 national standards setting processes by  
12 foreign countries that pose a national secu-  
13 rity risk; and

14 (iv) progress implementing the com-  
15 prehensive, long-term strategic plan devel-  
16 oped under paragraph (3).

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

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

22 (1) without regard to the civil service laws, em-  
23 ploy, and fix the compensation of, such specialists  
24 and other experts as may be necessary for the Direc-  
25 tor to carry out the functions of the Director; and

1           (2) subject to the civil service laws, employ such  
2 other officers and employees as may be necessary to  
3 carry out the functions of the Director.

4 (e) ANNUAL REPORT.—

5           (1) IN GENERAL.—Not less frequently than  
6 once each year, the Director shall submit to Con-  
7 gress a report on—

8                   (A) the activities of the Office; and

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

11           (2) FORM.—Each report submitted under para-  
12 graph (1) shall be submitted in unclassified form,  
13 but may include a classified annex.

14 (f) CONFORMING AMENDMENT.—Section 101(c) of  
15 the National Security Act of 1947 (50 U.S.C. 3021(c))  
16 is amended by inserting “the Director of the Office of  
17 Critical Technologies and Security,” after “Treasury,”.

18 **SEC. 3. COUNCIL ON CRITICAL TECHNOLOGIES AND SECU-**  
19 **RITY.**

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

23           (b) FUNCTION.—The function of the Council shall be  
24 to advise the President on matters relating to challenges

1 posed by foreign powers with respect to technology acqui-  
2 sition and transfer.

3 (c) MEMBERSHIP.—

4 (1) COMPOSITION.—The Council shall be com-  
5 posed of the following:

6 (A) The Director of the Office of Critical  
7 Technologies and Security appointed under sec-  
8 tion 2(b)(1).

9 (B) The Secretary of Agriculture.

10 (C) The Secretary of Commerce.

11 (D) The Secretary of Defense.

12 (E) The Secretary of Education.

13 (F) The Secretary of Energy.

14 (G) The Secretary of Homeland Security.

15 (H) The Secretary of State.

16 (I) The Secretary of Transportation.

17 (J) The Secretary of the Treasury.

18 (K) The Director of the Office of Manage-  
19 ment and Budget.

20 (L) The Director of National Intelligence.

21 (M) The Director of the Central Intel-  
22 ligence Agency.

23 (N) The Director of the Federal Bureau of  
24 Investigation.

1 (O) The United States Trade Representa-  
2 tive.

3 (P) The Director of the National Economic  
4 Council.

5 (Q) The National Security Advisor.

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

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

12 (T) The Ambassador to the United Na-  
13 tions.

14 (U) The Chair of the Federal Communica-  
15 tions Commission.

16 (V) The Chair of the Federal Trade Com-  
17 mission.

18 (W) Such other heads of departments and  
19 agencies of the Federal Government as the  
20 chairperson of the Council considers appro-  
21 priate.

22 (2) CHAIRPERSON.—The chairperson of the  
23 Council shall be the Director of the Office of Critical  
24 Technologies and Security appointed under section  
25 2(b)(1).

1 (d) CONSULTATION AND COOPERATION.—The Coun-  
2 cil—

3 (1) may constitute such advisory committees  
4 and may consult with such representatives of indus-  
5 try, agriculture, labor, consumers, State and local  
6 governments, and other groups, as the Council con-  
7 siders advisable;

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

10 (3) shall seek and obtain the cooperation of the  
11 various executive and independent agencies of the  
12 Federal Government in the development of special-  
13 ized studies essential to its responsibilities.

○