

116TH CONGRESS  
1ST SESSION

# H. R. 618

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

---

## IN THE HOUSE OF REPRESENTATIVES

JANUARY 16, 2019

Mr. RUPPERSBERGER (for himself, Mr. CONAWAY, Mr. HIMES, and Mr. HURD of Texas) introduced the following bill; which was referred to the Committee on Foreign Affairs, and in addition to the Committees on Armed Services, and Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## 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       lacks—

7               (1) an office in the Executive Office of the  
8       President that can coordinate security policy relating

1 to critical emerging, foundational, and dual-use tech-  
2 nologies between the National Security Council and  
3 the National Economic Council and that can inter-  
4 face with international, Federal, State, and local en-  
5 tities on that policy; and

6 (2) a strategic plan—

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

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

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

18 (1) to coordinate a whole-of-government re-  
19 sponse to protect critical emerging, foundational,  
20 and dual-use technologies and to effectively enlist  
21 the support of Federal agencies, the private sector,  
22 and other scientific and technical hubs, including  
23 academia, to support and assist with such response;  
24 and

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

6 **SEC. 2. OFFICE OF CRITICAL TECHNOLOGIES AND SECUR-**  
7 **RITY.**

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

12          (b) **DIRECTOR.**—

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

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

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

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

1 (B) be a Deputy Director for the National  
2 Economic Council and serve as a member of  
3 such council; and

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

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

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

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

15 (i) to stop the transfer of critical  
16 emerging, foundational, and dual-use tech-  
17 nologies to countries that pose a national  
18 security risk, including by leading the  
19 interagency process to identify emerging  
20 and foundational technologies under sec-  
21 tion 1758 of the John S. McCain National  
22 Defense Authorization Act for Fiscal Year  
23 2019 (Public Law 115–232); and

24 (ii) to maintain United States techno-  
25 logical leadership with respect to critical

1 emerging, foundational, and dual-use tech-  
2 nologies and ensure supply chain integrity  
3 and security for such technologies.

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

9 (C) To facilitate coordination and consulta-  
10 tion with—

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

17 (ii) the private sector, including indus-  
18 try, labor, consumer, and other groups as  
19 necessary;

20 (iii) other nongovernmental scientific  
21 and technical hubs and stakeholders, in-  
22 cluding academic stakeholders; and

23 (iv) United States allies and other de-  
24 fense partners.

1           (2) MESSAGING AND OUTREACH.—To lead mes-  
2           saging and outreach efforts by the Federal Govern-  
3           ment on the national security threat posed by the  
4           improper acquisition and transfer of critical emerg-  
5           ing, foundational, and dual-use technologies that the  
6           Federal Government determines necessary to pro-  
7           tect, by countries of concern including—

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

11                  (B) encouraging Federal agencies to work  
12                  with key stakeholders as described in paragraph  
13                  (1), as well as States, localities, international  
14                  partners, and allies, to better analyze and dis-  
15                  seminate critical information from the intel-  
16                  ligence community (as defined in section 3 of  
17                  the National Security Act of 1947 (50 U.S.C.  
18                  3003)); and

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

23                          (i) the improper acquisition and trans-  
24                          fer of critical emerging, foundational, and

1 dual-use technologies by countries that  
2 pose a national security risk; and

3 (ii) reliance on foreign products iden-  
4 tified by the Federal Government that pose  
5 a national security risk in private sector  
6 supply chains.

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

11 (A) to enhance the interagency process for  
12 identifying emerging and foundational tech-  
13 nologies carried out under section 1758 of the  
14 John S. McCain National Defense Authoriza-  
15 tion Act for Fiscal Year 2019 (Public Law  
16 115–232) and to re-evaluate those identifica-  
17 tions on an ongoing basis;

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

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

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

4 (iv) to address other security concerns re-  
5 lated to forced or unfair technology transfer to  
6 and from such countries;

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

13 (D) to develop specific policies and actions  
14 to enforce intellectual property and cybersecuri-  
15 ty standards to deter and prosecute industrial  
16 espionage and other similar measures; and

17 (E) to develop specific policies—

18 (i) to improve the research and devel-  
19 opment ecosystem, including academic in-  
20 stitutions, nonprofit organizations, and pri-  
21 vate entities; and

22 (ii) to reestablish the United States as  
23 the world leader in research and develop-  
24 ment; and



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

4 (4) MONITORING AND TRACKING.—

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

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

14 (ii) key trends relating to United  
15 States Government investments in innova-  
16 tion and competitiveness compared to gov-  
17 ernments of other countries;

18 (iii) inappropriate influence of inter-  
19 national standards setting processes by  
20 foreign countries that pose a national secu-  
21 rity risk; and

22 (iv) progress implementing the com-  
23 prehensive, long-term strategic plan devel-  
24 oped under paragraph (3).

1           (B) GOALS.—To monitor and track  
2 progress, using specific measures developed by  
3 the Office, made towards achieving goals relat-  
4 ing to protecting the security of critical emerg-  
5 ing, foundational, and dual-use technologies of  
6 the United States.

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

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

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

15 (e) ANNUAL REPORT.—

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

19           (A) the activities of the Office; and

20           (B) matters relating to national security  
21 and the protection of critical emerging,  
22 foundational, dual-use technologies.

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

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

5 **SEC. 3. COUNCIL ON CRITICAL TECHNOLOGIES AND SECUR-**  
6 **RITY.**

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

10 (b) FUNCTION.—The function of the Council shall be  
11 to advise the President on matters relating to challenges  
12 posed by foreign powers with respect to technology acqui-  
13 sition and transfer.

14 (c) MEMBERSHIP.—

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

17 (A) The Director of the Office of Critical  
18 Technologies and Security appointed under sec-  
19 tion 2(b)(1).

20 (B) The Secretary of Agriculture.

21 (C) The Secretary of Commerce.

22 (D) The Secretary of Defense.

23 (E) The Secretary of Education.

24 (F) The Secretary of Energy.

25 (G) The Secretary of Homeland Security.

1 (H) The Secretary of State.

2 (I) The Secretary of Transportation.

3 (J) The Secretary of the Treasury.

4 (K) The Director of the Office of Manage-  
5 ment and Budget.

6 (L) The Director of National Intelligence.

7 (M) The Director of the Central Intel-  
8 ligence Agency.

9 (N) The Director of the Federal Bureau of  
10 Investigation.

11 (O) The United States Trade Representa-  
12 tive.

13 (P) The Director of the National Economic  
14 Council.

15 (Q) The National Security Advisor.

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

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

22 (T) The United States Ambassador to the  
23 United Nations.

24 (U) The Chair of the Federal Communica-  
25 tions Commission.

1           (V) The Chair of the Federal Trade Com-  
2 mission.

3           (W) Such other heads of Federal agencies  
4 as the chairperson of the Council considers ap-  
5 propriate.

6           (2) CHAIRPERSON.—The chairperson of the  
7 Council shall be the Director of the Office of Critical  
8 Technologies and Security appointed under section  
9 2(b)(1).

10          (d) CONSULTATION AND COOPERATION.—The Coun-  
11 cil—

12           (1) may constitute such advisory committees  
13 and may consult with such representatives of indus-  
14 try, agriculture, labor, consumers, State and local  
15 governments, and other groups, as the Council con-  
16 siders advisable;

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

19           (3) shall seek and obtain the cooperation of ex-  
20 ecutive agencies, including independent agencies, of  
21 the Federal Government in the development of spe-  
22 cialized studies essential to its responsibilities.

○