

116TH CONGRESS  
1ST SESSION

# S. 2316

To require a plan for strengthening the supply chain intelligence function, to establish a National Supply Chain Intelligence Center, and for other purposes.

---

## IN THE SENATE OF THE UNITED STATES

JULY 30, 2019

Mr. CRAPO (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Select Committee on Intelligence

---

## A BILL

To require a plan for strengthening the supply chain intelligence function, to establish a National Supply Chain Intelligence Center, 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. SHORT TITLE.**

4 This Act may be cited as the “Manufacturing, Invest-  
5 ment, and Controls Review for Computer Hardware, Intel-  
6 lectual Property, and Supply Act of 2019” or the  
7 “MICROCHIPS Act of 2019”.

1 **SEC. 2. FINDINGS AND SENSE OF CONGRESS.**

2 (a) FINDINGS.—Congress makes the following find-  
3 ings:

4 (1) Fifth generation telecommunications tech-  
5 nology (commonly referred to as “5G”), as well as  
6 other emerging technologies, will revolutionize the  
7 technology industry, becoming a vital part of day-to-  
8 day business and life, and requires secure supply  
9 chains for the national security of the United States.

10 (2) An insecure supply chain for products sup-  
11 plied to the United States Government can lead to  
12 a degradation of critical infrastructure and tech-  
13 nology items that are essential to the defense of the  
14 United States.

15 (3) The United States Government confronts  
16 adversaries who seek to offset the military strength  
17 of the United States through asymmetric, nonkinetic  
18 actions that compromise and neutralize the decision-  
19 making systems, processes, and warfighting capabili-  
20 ties of the United States.

21 (4) These adversaries take advantage of the  
22 open and democratic system of the United States  
23 that prioritizes governmental transparency to con-  
24 nect citizens with the actions of the Government.

1           (5) The National Defense Strategy identified  
2           Russia and China as primary strategic competitors  
3           of the United States.

4           (6) Russia and China seek to steal sensitive de-  
5           fense information from the United States through  
6           the use of blended espionage operations in the sup-  
7           ply chain, supply chain activities, and cyberspace,  
8           and through insider threat human actors.

9           (7) The actions of Russia and China go well be-  
10          yond theft of critical military technology, threatening  
11          the integrity and readiness of information and weap-  
12          ons systems and potentially enabling key elements of  
13          the strategies of an adversary to defeat the Armed  
14          Forces of the United States across the spectrum of  
15          conflict.

16          (8) According to some estimates, cybersecurity  
17          spending in the United States from 2017 to 2021  
18          will exceed \$1,000,000,000,000 among the public  
19          and private sectors.

20          (9) Even with these large investments in cyber-  
21          security, the United States remains vulnerable to ad-  
22          vanced cyber actors like Russia and China.

23          (10) Since 2013, more than 6,000,000 indi-  
24          vidual data records have been compromised every

1 day through data breaches, with nearly half of these  
2 losses occurring in the Government sector.

3 (11) Large expenditures of resources and a pro-  
4 tective strategy that relies on firewalls and bound-  
5 aries that can be breached by a persistent actor are  
6 clearly insufficient and completely ignore the supply  
7 chain vector.

8 (12) Military weapons systems are not immune  
9 to cyber vulnerabilities.

10 (13) An October 2018 Government Account-  
11 ability Office report found that nearly all weapons  
12 systems of the United States have cyber  
13 vulnerabilities the scale of which the Department of  
14 Defense is “just beginning to grapple with”.

15 (14) Furthermore, the report stated that de-  
16 spite multiple warnings since the early 1990s, “cy-  
17 bersecurity has not been a focus of weapon systems  
18 acquisitions”.

19 (15) There have been numerous press stories  
20 about data breaches and theft of United States sen-  
21 sitive technology that prove that cyber vulnerabilities  
22 are real and not theoretical.

23 (16) The Department of Defense will spend  
24 more than \$1,600,000,000,000 to develop and field  
25 its current portfolio of weapons systems.

1           (17) Conducting acquisitions without making  
2 security resiliency a key discriminator in capability  
3 development and contract award decisions could po-  
4 tentially lead to additional losses of technological ad-  
5 vantages of the Armed Forces and negate efforts to  
6 improve the capabilities of the Armed Forces to  
7 meet the National Defense Strategy.

8           (18) Software, hardware, and services supply  
9 chains have proven to be major means through  
10 which adversaries seek to gain access to weapons  
11 systems and information and communications tech-  
12 nology platforms and systems of the United States.

13           (19) Vulnerabilities in these critical areas intro-  
14 duce unacceptable risks to human life and the ability  
15 of the Armed Forces to execute the missions the  
16 public of the United States expects of them.

17           (20) The establishment of the Protecting Crit-  
18 ical Technology Task Force of the Department of  
19 Defense and the Information and Communication  
20 Technology Supply Chain Risk Management Task  
21 Force of the Department of Homeland Security is a  
22 welcome first step, but the United States Govern-  
23 ment requires a fundamental security culture  
24 change.

1           (21) The innovative technologies that will help  
2 the Armed Forces, economy, and industry of the  
3 United States maintain competitive advantages over  
4 the competitors of the United States are developed  
5 in private industry and in academia.

6           (22) Engagement to find solutions with indus-  
7 try stakeholders and allied countries to mitigate the  
8 clear, present, and rapidly evolving threats to the  
9 national security of the United States is necessary.

10          (23) A national center to unify efforts across  
11 the whole of government to strategically warn of and  
12 support the mitigation of threats to supply chains  
13 and supply chain activities is vital to the cybersecu-  
14 rity, critical infrastructure, and national security of  
15 the United States.

16          (b) SENSE OF CONGRESS.—It is the sense of Con-  
17 gress that—

18           (1) the United States Government should en-  
19 deavor to deliver warfighting capabilities to oper-  
20 ational forces without having critical information or  
21 technology wittingly or unwittingly lost, stolen, or  
22 modified;

23           (2) the Department of Defense and the whole  
24 of the United States Government should adapt to  
25 the challenges presented by adversaries while main-

1 taining as much transparency with the people of the  
2 United States as possible;

3 (3) stronger effort should be placed on securing  
4 the vast supply chains of the contractors responsible  
5 for developing and producing the defense related ca-  
6 pabilities of the United States;

7 (4) the efforts of the Department of Defense,  
8 the Department of Homeland Security, and the Fed-  
9 eral Acquisition Security Council to protect critical  
10 technologies should be action oriented with clear out-  
11 come expectations and chains of accountability;

12 (5) technology protection should begin long be-  
13 fore a contract is signed between a contractor and  
14 the United States Government;

15 (6) the United States Government should im-  
16 prove its ability to collaborate to protect both the  
17 open research environment and emerging military  
18 technologies; and

19 (7) the United States Government should focus  
20 on supply chain security to ensure that military sys-  
21 tems and systems required for sensitive activities are  
22 not acquired or operated in a compromised state.

1 **SEC. 3. PLAN FOR STRENGTHENING THE SUPPLY CHAIN IN-**  
2 **TELLIGENCE FUNCTION.**

3 (a) IN GENERAL.—Not later than 180 days after the  
4 date of the enactment of this Act, the Director of the Na-  
5 tional Counterintelligence and Security Center, in coordi-  
6 nation with the Director of the Defense Counterintel-  
7 ligence and Security Agency and other interagency part-  
8 ners, shall submit to Congress a plan for strengthening  
9 the supply chain intelligence function.

10 (b) ELEMENTS.—The plan submitted under sub-  
11 section (a) shall address the following:

12 (1) Such recommendations as the Director of  
13 the National Counterintelligence and Security Cen-  
14 ter may have with respect to—

15 (A) the appropriate workforce model, in-  
16 cluding size, mix, and seniority, from the ele-  
17 ments of the intelligence community and other  
18 interagency partners; and

19 (B) the appropriate governance structure  
20 within the intelligence community and with  
21 interagency partners.

22 (2) The budgetary resources necessary to imple-  
23 ment the plan.

24 (3) The authorities necessary to implement the  
25 plan.

1 (c) DEFINITION OF INTELLIGENCE COMMUNITY.—In  
 2 this section, the term “intelligence community” has the  
 3 meaning given such term in section 3 of the National Se-  
 4 curity Act of 1947 (50 U.S.C. 3003).

5 **SEC. 4. ESTABLISHMENT OF NATIONAL SUPPLY CHAIN IN-**  
 6 **TELLIGENCE CENTER.**

7 (a) ESTABLISHMENT OF CENTER.—Title IX of the  
 8 Intelligence Authorization Act for Fiscal Year 2003 (50  
 9 U.S.C. 3382 et seq.) is amended by adding at the end  
 10 the following:

11 **“SEC. 905. NATIONAL SUPPLY CHAIN INTELLIGENCE CEN-**  
 12 **TER.**

13 “(a) ESTABLISHMENT OF CENTER.—There is within  
 14 the National Counterintelligence and Security Center in  
 15 the Office of the Director of National Intelligence a Na-  
 16 tional Supply Chain Intelligence Center.

17 “(b) DIRECTOR OF NATIONAL SUPPLY CHAIN INTEL-  
 18 LIGENCE CENTER.—There is a Director of the National  
 19 Supply Chain Intelligence Center, who shall be appointed  
 20 by the President, in consultation with the Director of Na-  
 21 tional Intelligence and other interagency partners as the  
 22 President considers appropriate.

23 “(c) CENTER PERSONNEL.—

24 “(1) SENIOR MANAGEMENT.—The Director of  
 25 the National Supply Chain Intelligence Center shall

1 ensure that the senior management of the Center in-  
2 cludes one or more detailees from each of the fol-  
3 lowing:

4 “(A) The Department of Defense.

5 “(B) The Department of Justice.

6 “(C) The Department of Homeland Secu-  
7 rity.

8 “(D) The Department of Commerce.

9 “(2) DETAIL OR ASSIGNMENT OF PER-  
10 SONNEL.—

11 “(A) IN GENERAL.—With the approval of  
12 the Director of the Office of Management and  
13 Budget, and in consultation with the congress-  
14 sional committees of jurisdiction, the Director  
15 of the National Supply Chain Intelligence Cen-  
16 ter may request of the head of any department,  
17 agency, or element of the Federal Government  
18 the detail or assignment of personnel from such  
19 department, agency, or element to the National  
20 Supply Chain Intelligence Center.

21 “(B) DUTIES.—Personnel detailed or as-  
22 signed under subparagraph (A) shall assist the  
23 National Supply Chain Intelligence Center in  
24 carrying out the primary missions of the Cen-  
25 ter.

1           “(C) TERMS.—Personnel detailed or as-  
2           signed under subparagraph (A) shall be as-  
3           signed or detailed to the National Supply Chain  
4           Intelligence Center for a period of not more  
5           than 2 years.

6           “(D) REGULAR EMPLOYMENT.—Any Fed-  
7           eral Government employee detailed or assigned  
8           under subparagraph (A) shall retain the rights,  
9           status, and privileges of his or her regular em-  
10          ployment without interruption.

11          “(d) PRIMARY MISSIONS.—The primary missions of  
12          the National Supply Chain Intelligence Center shall be as  
13          follows:

14               “(1) To aggregate all-source intelligence relat-  
15               ing to supply chains, including—

16                       “(A) classified and unclassified informa-  
17                       tion;

18                       “(B) threat information; and

19                       “(C) proprietary and sensitive information,  
20                       including risk and vulnerability information,  
21                       voluntarily provided by private entities.

22               “(2) To share strategic warnings relating to  
23               supply chains or supply chain activities, as the Di-  
24               rector of the National Supply Chain Intelligence  
25               Center considers appropriate and consistent with se-

1 security standards for classified information and sen-  
2 sitive proprietary information, among—

3 “(A) the elements of the intelligence com-  
4 munity (as defined in section 3 of the National  
5 Security Act of 1947 (50 U.S.C. 3003)), com-  
6 ponents of the Department of Justice and the  
7 Department of Defense, the Federal Acquisition  
8 Security Council, and other Federal agencies;

9 “(B) at-risk industry partners; and

10 “(C) governments of countries that are al-  
11 lies of the United States.

12 “(3) To serve as the central and shared knowl-  
13 edge resource for—

14 “(A) known and suspected threats to sup-  
15 ply chain activities or supply chain integrity  
16 from international groups, companies, coun-  
17 tries, or other entities; and

18 “(B) the goals, strategies, capabilities, and  
19 networks of contacts and support of such  
20 groups, companies, countries, and other enti-  
21 ties.

22 “(4) To perform tasks assigned to the National  
23 Supply Chain Intelligence Center by relevant Gov-  
24 ernment supply chain task forces, councils, including

1 the Federal Acquisition Security Council, and other  
2 entities.

3 “(e) ANNUAL REPORTS REQUIRED.—The Director of  
4 the National Supply Chain Intelligence Center shall annu-  
5 ally submit to Congress a report, with classified annexes  
6 as appropriate, on the state of threats to the security of  
7 supply chains and supply chain activities for United States  
8 Government acquisitions and replenishment as of the date  
9 of the submittal of the report.

10 “(f) FUNDING.—Amounts used to carry out this sec-  
11 tion shall be derived from amounts appropriated or other-  
12 wise made available for the National Intelligence Program  
13 (as defined in section 3 of the National Security Act of  
14 1947 (50 U.S.C. 3003)).”.

15 (b) CLERICAL AMENDMENT.—The table of contents  
16 in section 1(b) of such Act is amended by inserting after  
17 the item relating to section 904 the following new item:

“Sec. 905. National Supply Chain Intelligence Center.”.

18 (c) SENSE OF CONGRESS.—It is the sense of Con-  
19 gress that the Director of the National Supply Chain In-  
20 telligence Center should implement the recommendations  
21 submitted under section 3(b)(1).

1 **SEC. 5. INVESTMENT IN SUPPLY CHAIN SECURITY UNDER**  
2 **DEFENSE PRODUCTION ACT OF 1950.**

3 (a) IN GENERAL.—Section 303 of the Defense Pro-  
4 duction Act of 1950 (50 U.S.C. 4533) is amended by add-  
5 ing at the end the following:

6 “(h) INVESTMENT IN SUPPLY CHAIN SECURITY.—

7 “(1) IN GENERAL.—The President may make  
8 available to an eligible entity described in paragraph  
9 (2) payments to increase the security of supply  
10 chains and supply chain activities, if the President  
11 certifies to Congress not less than 30 days before  
12 making such a payment that the payment is in the  
13 national security interests of the United States.

14 “(2) ELIGIBLE ENTITY.—An eligible entity de-  
15 scribed in this paragraph is an entity that—

16 “(A) is organized under the laws of the  
17 United States or any jurisdiction within the  
18 United States; and

19 “(B) produces—

20 “(i) one or more critical components;

21 “(ii) critical technology; or

22 “(iii) one or more products for the in-  
23 creased security of supply chains or supply  
24 chain activities.

25 “(3) REGULATIONS.—

1           “(A) IN GENERAL.—Not later than 90  
2 days after the date of the enactment of the  
3 Manufacturing, Investment, and Controls Re-  
4 view for Computer Hardware, Intellectual Prop-  
5 erty, and Supply Act of 2019, the President  
6 shall prescribe regulations setting forth defini-  
7 tions for the terms ‘supply chain’ and ‘supply  
8 chain activities’ for the purposes of this sub-  
9 section.

10           “(B) SCOPE OF DEFINITIONS.—The defini-  
11 tions required by subparagraph (A)—

12           “(i) shall encompass—

13           “(I) the organization, people, ac-  
14 tivities, information, and resources in-  
15 volved in the delivery and operation of  
16 a product or service used by the Gov-  
17 ernment; or

18           “(II) critical infrastructure as de-  
19 fined in Presidential Policy Directive  
20 21 (February 12, 2013; relating to  
21 critical infrastructure security and re-  
22 silience); and

23           “(ii) may include variations for spe-  
24 cific sectors or Government functions.”.

○