116TH CONGRESS
1ST SESSION

S. _____

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

Mr. CRAPO introduced the following bill; which was read twice and referred to the Committee on _____

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.

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

SECTION 1. FINDINGS AND SENSE OF CONGRESS.

(a) FINDINGS.—Congress makes the following findings:

(1) Fifth generation telecommunications technology (commonly referred to as ''5G''), as well as other emerging technologies, will revolutionize the technology industry, becoming a vital part of day-to-

day business and life, and requires secure supply chains for the national security of the United States.

(2) An insecure supply chain for products supplied to the United States Government can lead to a degradation of critical infrastructure and technology items that are essential to the defense of the United States.

(3) The United States Government confronts adversaries who seek to offset the military strength of the United States through asymmetric, nonkinetic actions that compromise and neutralize the decision-making systems, processes, and warfighting capabilities of the United States.

(4) These adversaries take advantage of the open and democratic system of the United States that prioritizes governmental transparency to connect citizens with the actions of the Government.

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

(6) Russia and China seek to steal sensitive defense information from the United States through the use of blended espionage operations in the supply chain, supply chain activities, and cyberspace, and through insider threat human actors.

(7) The actions of Russia and China go well beyond theft of critical military technology, threatening the integrity and readiness of information and weapons systems and potentially enabling key elements of the strategies of an adversary to defeat the Armed Forces of the United States across the spectrum of conflict.

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

(9) Even with these large investments in cybersecurity, the United States remains vulnerable to advanced cyber actors like Russia and China.

(10) Since 2013, more than 6,000,000 individual data records have been compromised every day through data breaches, with nearly half of these losses occurring in the Government sector.

(11) Large expenditures of resources and a protective strategy that relies on firewalls and boundaries that can be breached by a persistent actor are clearly insufficient and completely ignore the supply chain vector.

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

(13) An October 2018 Government Accountability Office report found that nearly all weapons systems of the United States have cyber vulnerabilities the scale of which the Department of Defense is ''just beginning to grapple with''.

(14) Furthermore, the report stated that despite multiple warnings since the early 1990s, ''cybersecurity has not been a focus of weapon systems acquisitions''.

(15) There have been numerous press stories about data breaches and theft of United States sensitive technology that prove that cyber vulnerabilities are real and not theoretical.

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

(17) Conducting acquisitions without making security resiliency a key discriminator in capability development and contract award decisions could potentially lead to additional losses of technological advantages of the Armed Forces and negate efforts to improve the capabilities of the Armed Forces to meet the National Defense Strategy.

(18) Software, hardware, and services supply chains have proven to be major means through

which adversaries seek to gain access to weapons systems and information and communications technology platforms and systems of the United States.

(19) Vulnerabilities in these critical areas introduce unacceptable risks to human life and the ability of the Armed Forces to execute the missions the public of the United States expects of them.

(20) The establishment of the Protecting Critical Technology Task Force of the Department of Defense and the Information and Communication Technology Supply Chain Risk Management Task Force of the Department of Homeland Security is a welcome first step, but the United States Government requires a fundamental security culture change.

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

(22) Engagement to find solutions with industry stakeholders and allied countries to mitigate the clear, present, and rapidly evolving threats to the national security of the United States is necessary.

(23) A national center to unify efforts across the whole of government to strategically warn of and support the mitigation of threats to supply chains and supply chain activities is vital to the cybersecurity, critical infrastructure, and national security of the United States.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) the United States Government should endeavor to deliver warfighting capabilities to operational forces without having critical information or technology wittingly or unwittingly lost, stolen, or modified;

(2) the Department of Defense and the whole of the United States Government should adapt to the challenges presented by adversaries while maintaining as much transparency with the people of the United States as possible;

(3) stronger effort should be placed on securing the vast supply chains of the contractors responsible for developing and producing the defense related capabilities of the United States;

(4) the efforts of the Department of Defense, the Department of Homeland Security, and the Federal Acquisition Security Council to protect critical

technologies should be action oriented with clear outcome expectations and chains of accountability;

(5) technology protection should begin long before a contract is signed between a contractor and the United States Government;

(6) the United States Government should improve its ability to collaborate to protect both the open research environment and emerging military technologies; and

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

SEC. 2. PLAN FOR STRENGTHENING THE SUPPLY CHAIN INTELLIGENCE FUNCTION.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the National Counterintelligence and Security Center, in coordination with the Director of the Defense Counterintelligence and Security Agency and other interagency partners, shall submit to Congress a plan for strengthening the supply chain intelligence function.

(b) ELEMENTS.—The plan submitted under subsection (a) shall address the following:

(1) Such recommendations as the Director of the National Counterintelligence and Security Center may have with respect to—

(A) the appropriate workforce model, including size, mix, and seniority, from the elements of the intelligence community and other interagency partners; and

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

(2) The budgetary resources necessary to implement the plan.

(3) The authorities necessary to implement the plan.

(c) DEFINITION OF INTELLIGENCE COMMUNITY.—In this section, the term ''intelligence community'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 3. ESTABLISHMENT OF NATIONAL SUPPLY CHAIN INTELLIGENCE CENTER.

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

"SEC. 905. NATIONAL SUPPLY CHAIN INTELLIGENCE CENTER.

''(a) ESTABLISHMENT OF CENTER.—There is within the National Counterintelligence and Security Center in the Office of the Director of National Intelligence a National Supply Chain Intelligence Center.

''(b) DIRECTOR OF NATIONAL SUPPLY CHAIN INTELLIGENCE CENTER.—There is a Director of the National Supply Chain Intelligence Center, who shall be appointed by the President, in consultation with the Director of National Intelligence and other interagency partners as the President considers appropriate.

''(c) CENTER PERSONNEL.—

''(1) SENIOR MANAGEMENT.—The Director of the National Supply Chain Intelligence Center shall ensure that the senior management of the Center includes one or more detailees from each of the following:

''(A) The Department of Defense.

''(B) The Department of Justice.

''(C) The Department of Homeland Security.

''(D) The Department of Commerce.

''(2) DETAIL OR ASSIGNMENT OF PERSONNEL.—

''(A) IN GENERAL.—With the approval of the Director of the Office of Management and Budget, and in consultation with the congressional committees of jurisdiction, the Director of the National Supply Chain Intelligence Center may request of the head of any department, agency, or element of the Federal Government the detail or assignment of personnel from such department, agency, or element to the National Supply Chain Intelligence Center.

''(B) DUTIES.—Personnel detailed or assigned under subparagraph (A) shall assist the National Supply Chain Intelligence Center in carrying out the primary missions of the Center.

''(C) TERMS.—Personnel detailed or assigned under subparagraph (A) shall be assigned or detailed to the National Supply Chain Intelligence Center for a period of not more than 2 years.

''(D) REGULAR EMPLOYMENT.—Any Federal Government employee detailed or assigned under subparagraph (A) shall retain the rights, status, and privileges of his or her regular employment without interruption.

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

''(1) To aggregate all-source intelligence relating to supply chains, including—

''(A) classified and unclassified information;

''(B) threat information; and

''(C) proprietary and sensitive information, including risk and vulnerability information, voluntarily provided by private entities.

''(2) To share strategic warnings relating to supply chains or supply chain activities, as the Director of the National Supply Chain Intelligence Center considers appropriate and consistent with security standards for classified information and sensitive proprietary information, among—

''(A) the elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)), components of the Department of Justice and the Department of Defense, the Federal Acquisition Security Council, and other Federal agencies;

''(B) at-risk industry partners; and

"(C) governments of countries that are allies of the United States.

"(3) To serve as the central and shared knowledge resource for—

"(A) known and suspected threats to supply chain activities or supply chain integrity from international groups, companies, countries, or other entities; and

"(B) the goals, strategies, capabilities, and networks of contacts and support of such groups, companies, countries, and other entities.

"(4) To perform tasks assigned to the National Supply Chain Intelligence Center by relevant Government supply chain task forces, councils, including the Federal Acquisition Security Council, and other entities.

"(e) ANNUAL REPORTS REQUIRED.—The Director of the National Supply Chain Intelligence Center shall annually submit to Congress a report, with classified annexes as appropriate, on the state of threats to the security of supply chains and supply chain activities for United States Government acquisitions and replenishment as of the date of the submittal of the report.

''(f) FUNDING.—Amounts used to carry out this section shall be derived from amounts appropriated or otherwise made available for the National Intelligence Program (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)).''.

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

''Sec. 905. National Supply Chain Intelligence Center.''.

(c) SENSE OF CONGRESS.—It is the sense of Congress that the Director of the National Supply Chain Intelligence Center should implement the recommendations submitted under section 2(b)(1).

SEC. 4. INVESTMENT IN SUPPLY CHAIN SECURITY UNDER DEFENSE PRODUCTION ACT OF 1950.

(a) IN GENERAL.—Section 303 of the Defense Production Act of 1950 (50 U.S.C. 4533) is amended by adding at the end the following:

''(h) INVESTMENT IN SUPPLY CHAIN SECURITY.—

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

''(2) ELIGIBLE ENTITY.—An eligible entity described in this paragraph is an entity that—

''(A) is organized under the laws of the United States or any jurisdiction within the United States; and

''(B) produces—

''(i) one or more critical components;

''(ii) critical technology; or

''(iii) one or more products for the increased security of supply chains or supply chain activities.

''(3) REGULATIONS.—

''(A) IN GENERAL.—Not later than 90 days after the date of the enactment of this subsection, the President shall prescribe regulations setting forth definitions for the terms 'supply chain' and 'supply chain activities' for the purposes of this subsection.

''(B) SCOPE OF DEFINITIONS.—The definitions required by subparagraph (A)—

''(i) shall encompass—

''(I) the organization, people, activities, information, and resources involved in the delivery and operation of

a product or service used by the Government; or

''(II) critical infrastructure as defined in Presidential Policy Directive 21 (February 12, 2013; relating to critical infrastructure security and resilience); and

''(ii) may include variations for specific sectors or Government functions.''.