

117TH CONGRESS  
1ST SESSION

# H. R. 6169

To direct the Secretary of Defense to establish a framework relating to risks to the defense supply chain, and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 7, 2021

Ms. SLOTKIN (for herself and Mr. GALLAGHER) introduced the following bill; which was referred to the Committee on Armed Services

---

## A BILL

To direct the Secretary of Defense to establish a framework relating to risks to the defense supply chain, 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. DEFENSE SUPPLY CHAIN RISK ASSESSMENT**  
4 **FRAMEWORK.**

5 (a) IN GENERAL.—Not later than one year after the  
6 date of the enactment of this Act, the Secretary of Defense  
7 shall establish a framework, which may be included as part  
8 of a framework developed under section 2509 of title 10,  
9 United States Code, and pursuant to recommendations  
10 provided under section 5 of Executive Order 14017 (86

1 Fed. Reg. 11849, relating to America’s supply chains), to  
2 consolidate the information relating to risks to the defense  
3 supply chain that is collected by the elements of the De-  
4 partment of Defense to—

5 (1) enable Department-wide risk assessments of  
6 the defense supply chain; and

7 (2) support the development of strategies to  
8 mitigate risks to the defense supply chain.

9 (b) FRAMEWORK REQUIREMENTS.—The framework  
10 established under subsection (a) shall—

11 (1) provide for the collection, management, and  
12 storage of data from the supply chain risk manage-  
13 ment processes of the Department of Defense;

14 (2) provide for the collection of reports on sup-  
15 ply chain risk management from the military depart-  
16 ments and Defense Agencies, and the dissemination  
17 of such reports to the components of the military de-  
18 partments and Defense Agencies involved in the  
19 management of supply chain risk;

20 (3) enable all elements of the Department to  
21 analyze the information collected by such framework  
22 to identify risks to the defense supply chain;

23 (4) enable the Department to—

24 (A) assess the capabilities of foreign adver-  
25 saries (as defined in section 8(c) of the Secure

1 and Trusted Communications Networks Act of  
2 2019 (47 U.S.C. 1607(c)) to affect the defense  
3 supply chain;

4 (B) analyze the ability of the industrial  
5 base of the United States to meet the needs of  
6 the defense supply chain;

7 (C) track global technology trends that  
8 could affect the defense supply chain, as deter-  
9 mined by the Secretary of Defense; and

10 (D) assess the risks posed by emerging  
11 threats to the defense supply chain;

12 (5) support the identification of technology in  
13 which the Department may invest to reduce risks to  
14 the defense supply chain, including by improving the  
15 resilience of the defense supply; and

16 (6) provide for—

17 (A) a map of the supply chains for major  
18 end items that supports analysis, monitoring,  
19 and reporting with respect to high-risk sub-  
20 contractors and risks to such supply chain; and

21 (B) the use of a covered application de-  
22 scribed in subsection (c) in the creation of such  
23 map to assess risks to the supply chain for  
24 major end items by business sector, vendor,  
25 program, part, or technology.

1 (c) COVERED APPLICATION DESCRIBED.—The cov-  
2 ered application described in this subsection is a covered  
3 application that includes the following elements:

4 (1) A centralized database that consolidates  
5 multiple disparate data sources into a single reposi-  
6 tory to ensure the consistent availability of data.

7 (2) Centralized reporting to allow for efficient  
8 mitigation and remediation of identified supply chain  
9 vulnerabilities.

10 (3) Broad interoperability with other software  
11 and systems to ensure support for the analytical ca-  
12 pabilities of users across the Department.

13 (4) Scalable technology to support multiple  
14 users, access controls for security, and functionality  
15 designed for information-sharing and collaboration.

16 (d) GUIDANCE.—Not later than 180 days after the  
17 framework required under subsection (a) is established,  
18 and regularly thereafter, the Secretary of Defense shall  
19 issue guidance on mitigating risks to the defense supply  
20 chain.

21 (e) REPORTS.—

22 (1) PROGRESS REPORT.—Not later than 180  
23 days after the date of the enactment of this Act, the  
24 Secretary of Defense shall submit to the congres-  
25 sional defense committees a report on the progress

1 of establishing the framework as required under sub-  
2 section (a).

3 (2) FINAL REPORT.—Not later than one year  
4 after the date of the enactment of this Act, the Sec-  
5 retary of Defense shall submit to the congressional  
6 defense committees a report describing the frame-  
7 work established under subsection (a) and the orga-  
8 nizational structure to manage and oversee the  
9 framework.

10 (f) DEFINITIONS.—In this section:

11 (1) COVERED APPLICATION.—The term “cov-  
12 ered application” means a software-as-a-service ap-  
13 plication that uses decision science, commercial data,  
14 and machine learning techniques.

15 (2) DEFENSE AGENCY; MILITARY DEPART-  
16 MENT.—The terms “Defense Agency” and “military  
17 department” have the meanings given such terms in  
18 section 101 of title 10, United States Code.

19 (3) HIGH-RISK SUBCONTRACTORS.—The term  
20 “high-risk subcontractor” means a subcontractor at  
21 any tier that supplies major end items for the De-  
22 partment of Defense.

23 (4) MAJOR END ITEM.—The term “major end  
24 item” means an item subject to a unique item-level  
25 traceability requirement at any time in the life cycle

1 of such item under Department of Defense Instruc-  
2 tion 8320.04, titled “Item Unique Identification  
3 (IUID) Standards for Tangible Personal Property”  
4 and dated September 3, 2015, or any successor in-  
5 struction.

○