**Calendar No. 153**

| 117TH CONGRESS *1st Session* | SENATE | REPORT 117–43 |
|---|---|---|

# SUPPLY CHAIN SECURITY TRAINING ACT OF 2021

## R E P O R T

OF THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

## S. 2201

TO MANAGE SUPPLY CHAIN RISK THROUGH COUNTERINTELLIGENCE TRAINING, AND FOR OTHER PURPOSES

OCTOBER 26, 2021.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
29–010 WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
KATIE A. CONLEY, *Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
ANDREW C. DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*
JEREMY H. HAYES, *Minority Senior Professional Staff Member*
SAM J. MULOPULOS, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

**Calendar No. 153**

117TH CONGRESS *1st Session* | SENATE | REPORT 117–43

# SUPPLY CHAIN SECURITY TRAINING ACT OF 2021

OCTOBER 26, 2021.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

# R E P O R T

[To accompany S. 2201]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2201) to manage supply chain risk through counterintelligence training, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS



## I. PURPOSE AND SUMMARY

S. 2201, the Supply Chain Security Training Act of 2021, directs the General Services Administration (GSA) to develop a training program to prepare personnel at all federal agencies to identify and mitigate supply chain threats that arise during the acquisition of various products and services, including information and communications technology (ICT). Recent major cyber attacks and incidents involving outside vendors show that supply chains present serious challenges to the security of federal agencies and their information technology networks. There is, however, no government-wide supply chain security training that federal personnel must complete. This lack of standardized training puts federal agencies

and the American public at risk. Developing and implementing a standardized supply chain security training program for procurement and acquisitions personnel will allow federal agencies to better understand and mitigate threats and vulnerabilities in their supply chains. The training can be integrated into existing agency training processes and will include information on current threats and known vulnerabilities. S. 2201 will also make the training available to legislative and judicial branch officials.[1]

## II. BACKGROUND AND NEED FOR THE LEGISLATION

Federal agencies rely on global supply chains for a variety of goods and services vital to agency operations, and these supply chains are increasingly *vulnerable* to malicious actors and other threats.[2] The complexity of global supply chains, which can stretch across continents at every stage of a product's lifecycle, make them vulnerable to targeting by foreign governments, criminal actors, purveyors of counterfeit goods, and other actors.[3] For example, Russian cyber attacks using software sold by American vendor SolarWinds[4] and Chinese cyber attacks using Microsoft's Exchange software[5] compromised federal systems and data across numerous federal agencies.

In response to this growing threat, the Committee approved S. 3085, the Federal Acquisition Supply Chain Security Act of 2018, which was later signed into law as part of the SECURE Act.[6] This law established the Federal Acquisition Security Council.[7] The Council coordinates federal efforts related to supply chain security and created a process to exclude bad actors from the federal supply chain.[8] However, federal acquisition officials, who are responsible for and well trained in aspects of the Federal Acquisition Regulation and the general process for acquiring information technology goods and services, have little or no training regarding the potential counterintelligence risks posed by acquiring those same goods and services.[9]

S. 2201 addresses this concern by directing GSA to develop a training program to help all federal officials with supply chain risk management responsibilities identify and mitigate security threats that arise throughout the acquisition and procurement process. It requires the Office of Management and Budget (OMB) to promul-

---

[1] On May 15, 2019, the Committee approved S. 1388, the Supply Chain Counter-intelligence Act of 2019, which is similar to S. 2201. Accordingly, this committee report is in some respects similar to the committee report for S. 1388, S. Rept. No. 116–87.

[2] *See* Government Accountability Office, *Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* at 6–8 (GAO–21–171) (Dec. 2020).

[3] *See id.* at 9 and n.13.

[4] *See* National Cyber Security Centre, Cybersecurity and Infrastructure Agency, Federal Bureau of Investigation, and National Security Agency, *Advisory: Further TTPs Associated with SVR Cyber Actors* (May 7, 2021) (https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf).

[5] *See* White House: *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China* (July 19, 2021) (https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/).

[6] Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115–39 (2018).

[7] *Id.*

[8] *Id.*

[9] *Evanina: Root Out Supply Chain's Weak Links in Private Sector, Procurement Departments,* Homeland Security Today (Apr. 7, 2019) (https://www.hstoday.us/subject-matter-areas/cybersecurity/evanina-root-out-supply-chains-weak-links-in-private-sector-procurement-departments/).

gate guidance requiring executive agencies to adopt and use the training program and makes the guidance and training available to the legislative and judicial branches. It also requires GSA to report annually to Congress on the program's implementation for several years after enactment.

## III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 2201, the Supply Chain Security Training Act of 2021, on June 23, 2021 with Senator Ron Johnson (R–WI). The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. The Committee considered S. 2201 at a business meeting on July 14, 2021. During the business meeting, Senator Peters offered an amendment as modified to change "executive agency" to "federal agency," extend the definition of "federal agency" to include judicial and legislative branch offices, and require OMB to make its implementation guidance available to the legislative and judicial branches. The amendment, as modified, was adopted *en bloc* by voice vote with Senators Peters, Hassan, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present. The Committee ordered the bill, as amended, reported favorably *en bloc* by voice vote with Senators Peters, Hassan, Rosen, Padilla, Ossoff, Portman, Johnson, Lankford, Romney, Scott, and Hawley present.

## IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

*Section 1. Short title*

This section designates the short title of the bill as the "Supply Chain Security Training Act of 2021."

*Section 2. Training program to manage supply chain risk*

This Section establishes the training program.

Subsection (a) requires the GSA Administrator, through the Federal Acquisition Institute, to develop a training program for officials with supply chain risk management responsibilities at federal agencies not later than 180 days after enactment.

Subsection (b) specifies the content of the training, which will be designed to prepare personnel to perform supply chain risk management activities and identify and mitigate supply chain security threats that arise throughout the acquisition lifecycle, with a special emphasis on information and communications technology. The training program will also provide information relevant to current, specific supply chain security threats and will be updated as often as GSA determines necessary.

Subsection (c) mandates that the GSA Administrator coordinate with the Federal Acquisition Security Council, the Secretary of Homeland Security, and the Director of the Office of Personnel Management and consult with the Director of the Department of Defense's Defense Acquisition University and the Director of National Intelligence in developing the training program.

Subsection (d) requires the Director of OMB to promulgate guidance requiring executive agencies to adopt and use the training program. The guidance will allow executive agencies to incorporate the training program into existing agency training programs and instruct agencies on how to identify agency officials with supply

chain risk management responsibilities. Additionally, this subsection requires OMB to make the training and implementation guidance available to the legislative and judicial branches.

*Section 3. Reports on implementation of program*

This section requires GSA to submit a report to Congress on implementation of the training program, within 180 days of completing the first course and annually for the next three years.

*Section 4. Definitions*

This section defines "appropriate congressional committees and leadership," "information and communications technology," "executive agency," "federal agency," and "training program."

## V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

## VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
*Washington, DC, October 20, 2021.*

Hon. GARY C. PETERS,
*Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2201, the Supply Chain Security Training Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

PHILLIP L. SWAGEL,
*Director.*

Enclosure.

**S. 2201, Supply Chain Security Training Act of 2021**
**As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 14, 2021**

| By Fiscal Year, Millions of Dollars | 2022 | 2022-2026 | 2022-2031 |
|---|---|---|---|
| Direct Spending (Outlays) | 0 | 0 | 0 |
| Revenues | 0 | 0 | 0 |
| Increase or Decrease (-) in the Deficit | 0 | 0 | 0 |
| Spending Subject to Appropriation (Outlays) | * | * | not estimated |

| | | | |
|---|---|---|---|
| Statutory pay-as-you-go procedures apply? | No | **Mandate Effects** | |
| Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032? | No | Contains intergovernmental mandate? | No |
| | | Contains private-sector mandate? | No |

* = between zero and $500,000

S. 2201 would direct the General Services Administration (GSA) to develop a program to train federal employees in managing the risks to federal agencies' supply chains. GSA would coordinate the use of the program among federal agencies, detail the program's content, and report to the Congress on implementation.

Executive Order 14028, Improving the Nation's Cybersecurity, issued on May 12, 2021, and the Federal Acquisition Supply Chain Security Act of 2018 currently require agencies to assess and mitigate risks to their supply chains. In addition, the Federal Acquisition Institute and the Defense Acquisition University offer training and other resources for managing risk related to supply chains, and CBO expects that most federal employees who would be affected by the bill will take such training under current law. Thus, because the training required under the bill is available to federal agencies under current law, CBO expects that the provisions related to training would have no significant cost. Based on the cost of similar reports, CBO estimates that the reporting requirements would cost less than $500,000 over the 2022–2026 period.

The CBO staff contact for this estimate is Matthew Pickford. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

## VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.

○