LegiList

Congress, Made Clear.

Bill Fact Sheet – December 10, 2025
https://legilist.com
Bill page: https://legilist.com/bill/113/hr/5793

HR 5793

Cyber Supply Chain Management and Transparency Act of 2014

Congress: 113 (2013–2015, Ended)
Chamber: House
Policy Area: Government Operations and Politics
Introduced: Dec 4, 2014
Current Status: Referred to the House Committee on Oversight and Government Reform.
Latest Action: Referred to the House Committee on Oversight and Government Reform. (Dec 4, 2014)
Official Text: https://www.congress.gov/bill/113th-congress/house-bill/5793

Sponsor

Name: Rep. Royce, Edward R. [R-CA-39]
Party: Republican • **State:** CA • **Chamber:** House

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Jenkins, Lynn [R-KS-2]	R · KS		Dec 4, 2014

Committee Activity

Committee	Chamber	Activity	Date
Oversight and Government Reform Committee	House	Referred To	Dec 4, 2014

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

No related bills are listed.

Summary (as of Dec 4, 2014)

Cyber Supply Chain Management and Transparency Act of 2014 - Requires the Office of Management and Budget (OMB) to issue guidelines for agencies that contract to acquire software, firmware, or products containing a third party or open source binary component.

Requires binary component contracts to include clauses requiring:

- a confidentially supplied list, or a bill of materials, of each binary component that is used in the software, firmware, or product;
- the contractor to verify that products do not contain known security vulnerabilities and to notify the purchasing agency of any known vulnerabilities or defects;
- the contractor to obtain a waiver from the purchasing agency for components known to be vulnerable;
- an agency approving a vulnerability waiver to accept all risk associated with component use;
- product designs to allow fixes with patches, updates, or replacements; and
- the contractor to provide timely repairs for discovered vulnerabilities.

Directs the OMB to issue guidance requiring agencies: (1) to replace components with currently known vulnerabilities and to remove or repair any new vulnerable components that become known; and (2) to migrate to patchable, repairable, and fixable products.

Requires agencies to provide the Department of Homeland Security (DHS) with a list of each known vulnerable component in any product in use by the agencies.

Directs DHS to issue an annual confidential report describing the security vulnerabilities of projects that created any known vulnerable component. Requires the report to assess the integrity of component suppliers for the incidence of security vulnerabilities for use by other agencies.

Requires agencies, within 30 months after enactment of this Act, to report to Congress regarding the completion of the removal of each known vulnerable or defective component.

Directs other entities of the U.S. government to replace vulnerable components with less vulnerable alternatives.

Actions Timeline

- **Dec 4, 2014:** Introduced in House
- **Dec 4, 2014:** Sponsor introductory remarks on measure. (CR E1743-1745)
- **Dec 4, 2014:** Referred to the House Committee on Oversight and Government Reform.