AMENDMENT TO RULES COMM. PRINT 117–13

OFFERED BY MR. TORRES OF NEW YORK

At the end of subtitle D of title XV, add the following new section:

SEC. 15. DEPARTMENT OF HOMELAND SECURITY

GUIDANCE WITH RESPECT TO CERTAIN INFORMATION AND COMMUNICATIONS TECHNOLOGY OR SERVICES CONTRACTS.

(a) GUIDANCE.—The Secretary of Homeland Security, acting through the Under Secretary, shall issue guidance with respect to new and existing covered contracts.

(b) NEW COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each new covered contract, as a condition on the award of such a contract, each contractor responding to a solicitation for such a contract shall submit to the covered officer—

(1) a planned bill of materials when submitting a bid proposal; and

(2) the certification and notifications described in subsection (e).

(c) EXISTING COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each exist-
ing covered contract, each contractor with an existing covered contract shall submit to the covered officer—

(1) the bill of materials used for such contract, upon the request of such officer; and

(2) the certification and notifications described in subsection (e).

(d) Updating Bill of Materials.—With respect to a covered contract, in the case of a change to the information included in a bill of materials submitted pursuant to subsections (b)(1) and (c)(1), each contractor shall submit to the covered officer the update to such bill of materials, in a timely manner.

(e) Certification and Notifications.—The certification and notifications referred to in subsections (b)(2) and (c)(2), with respect to a covered contract, are the following:

(1) A certification that each item listed on the submitted bill of materials is free from all known vulnerabilities or defects affecting the security of the end product or service identified in—

(A) the National Institute of Standards and Technology National Vulnerability Database; and

(B) any database designated by the Under Secretary, in coordination with the Director of
the Cybersecurity and Infrastructure Security Agency, that tracks security vulnerabilities and defects in open source or third-party developed software.

(2) A notification of each vulnerability or defect affecting the security of the end product or service, if identified, through—

(A) the certification of such submitted bill of materials required under paragraph (1); or

(B) any other manner of identification.

(3) A notification relating to the plan to mitigate, repair, or resolve each security vulnerability or defect listed in the notification required under paragraph (2).

(f) ENFORCEMENT.—In developing guidance under subsection (a), the Secretary shall instruct covered officers with respect to—

(1) the processes available to such officers enforcing subsections (b) and (c); and

(2) when such processes should be used.

(g) EFFECTIVE DATE.—The guidance required under subsection (a) shall take effect on the date that is 180 days after the date of the enactment of this section.

(h) GAO REPORT.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General
of the United States shall submit to the Secretary, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes—

(1) a review of the implementation of this section;

(2) information relating to the engagement of the Department of Homeland Security with industry;

(3) an assessment of how the guidance issued pursuant to subsection (a) complies with Executive Order 14208 (86 Fed. Reg. 26633; relating to improving the nation’s cybersecurity); and

(4) any recommendations relating to improving the supply chain with respect to covered contracts.

(i) DEFINITIONS.—In this section:

(1) The term “bill of materials” means a list of the parts and components (whether new or reused) of an end product or service, including, with respect to each part and component, information relating to the origin, composition, integrity, and any other information as determined appropriate by the Under Secretary.
(2) The term “covered contract” means a contract relating to the procurement of covered information and communications technology or services for the Department.

(3) The term “covered information and communications technology or services” means the terms—

(A) “information technology” (as such term is defined in section 11101(6) of title 40, United States Code);

(B) “information system” (as such term is defined in section 3502(8) of title 44, United States Code);

(C) “telecommunications equipment” (as such term is defined in section 3(52) of the Communications Act of 1934 (47 U.S.C. 153(52))); and

(D) “telecommunications service” (as such term is defined in section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53))).

(4) The term “covered officer” means—

(A) a contracting officer of the Department; and

(B) any other official of the Department as determined appropriate by the Under Secretary.

(6) The term “software” means computer programs and associated data that may be dynamically written or modified during execution.

(7) The term “Under Secretary” means the Under Secretary for Management of the Department.