

**AMENDMENT TO RULES COMMITTEE PRINT 119-33 OFFERED BY MRS. BIGGS
OF SOUTH CAROLINA**

(a) Department of Defense Audit.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall initiate a Department-wide audit to identify the presence of covered cellular modules within covered systems.

(2) SCOPE.—The audit required under paragraph (1) shall—

(A) cover all military departments, combatant commands, defense agencies, and Department of Defense activities or programs;

(B) prioritize covered systems critical to military mobility, logistics, and installation security;

(C) include both government-owned and contractor-operated covered systems connected to Department of Defense networks or accessing Department of Defense information;

(D) identify to the maximum extent practicable, the manufacturer, model, firmware version, and host product for each covered cellular module identified; and

(E) assess the cybersecurity risk posed by each identified covered cellular module, including data flows, network exposure, and potential for remote access.

(b) Mitigation and Reporting.—

(1) REPORT REQUIRED.—Not later than 1 year after the date of the enactment of this Act, and biennially thereafter for a period not to exceed 6 years, the Secretary shall submit to the congressional defense committees a report on the audit and mitigation activities carried out under this section.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) The preliminary or updated findings of the audit required under subsection (b).

(B) A description of ongoing and planned mitigation measures, including—

(i) rip-and-replace programs;

(ii) accelerated divestiture or retirement of legacy assets;

(iii) network segmentation, isolation, or compensating cybersecurity or engineering controls;

(iv) firmware or software remediation; and

(v) supply-chain substitution with trusted alternatives.

(C) Cost estimates, timelines, and resource requirements for each category of mitigation measure described in subparagraph (B).

(D) An identification of any statutory, regulatory, or acquisition barriers to completing mitigation.

(E) Recommendations for additional legislative authorities, if any, needed to

complete mitigation.

(3) FORM.—Each report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) Comptroller General Report.—Not later than 180 days after the submission of the report required in subsection (b), the Comptroller General of the United States shall submit to the congressional defense committees a report on the implementation and effectiveness of the activities described in subsection (b).

(d) Definitions.—In this section:

(1) CELLULAR MODULE.—The term “cellular module” means a modular transmitter, as described in section 15.212 of title 47, Code of Federal Regulations, that provides cellular connectivity to a host product, including an Internet of things device.

(2) COVERED CELLULAR MODULE.—The term “covered cellular module” means any cellular module produced, manufactured, or provided by—

(A) an entity identified under section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 41 U.S.C. 3901 note prec.);

(B) an entity that is owned by, controlled by, or subject to the jurisdiction or direction of the People’s Republic of China; or

(C) any other entity determined by the Secretary of Defense to present an unacceptable supply-chain risk.

(3) COVERED SYSTEM.—The term “covered system” means any item of infrastructure owned, leased, operated, or controlled by the Department of Defense.

(4) INTERNET OF THINGS DEVICE.—The term “Internet of things device” has the meaning given to such term in NIST Special Publication 1800–16.