AMENDMENT TO RULES COMM. PRINT 117–31
OFFERED BY MR. LANGEVIN OF RHODE ISLAND

Add at the end of division F the following:

SEC. 50105. CRITICAL TECHNOLOGY SECURITY CENTERS.

(a) CRITICAL TECHNOLOGY SECURITY CENTERS.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.) is amended by adding at the end the following new section:

"SEC. 323. CRITICAL TECHNOLOGY SECURITY CENTERS.

''(a) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Under Secretary for Science and Technology, and in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall award grants, contracts, or cooperative agreements to covered entities for the establishment of not fewer than four cybersecurity-focused Critical Technology Security Centers to evaluate and test the security of devices and technologies that underpin national critical functions.

''(b) INITIAL CENTERS.—With respect to the Critical Technology Security Centers referred to in subsection (a), four of such centers shall be as follows:

''(1) The Center for Network Technology Security, to study the security of information and communications technology that underpins national critical functions related to communications.

''(2) The Center for Connected Industrial Control System Security, to study the security of connected programmable data logic controllers, supervisory control and data acquisition servers, and other networked industrial equipment.

''(3) The Center for Open Source Software Security, to study vulnerabilities in open source software used to support national critical functions.

''(4) The Center for Federal Critical Software Security, to study the security of software used by the Federal Government that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources).

''(c) ADDITIONAL CENTERS.—The Under Secretary may, in coordination with the Director, award grants, contracts, or cooperative agreements to covered entities for the establishment of additional Critical Technology Security Centers to address technologies vital to national critical functions.

''(d) SELECTION OF CRITICAL TECHNOLOGIES.—Before awarding a grant, contract, or cooperative agreement to a covered entity to establish a Critical Technology Security Center, the Under Secretary shall consult with the Director, who shall provide the Under Secretary a list of technologies within the remit of the center that support national critical functions.

''(e) RESPONSIBILITIES.—In studying the security of technologies within its remit, each center shall have the following responsibilities:

''(1) Conducting rigorous security testing to identify vulnerabilities in such technologies.

''(2) Reporting new vulnerabilities found and the tools, techniques, and practices used to uncover such vulnerabilities to the developers of such technologies in question and to the Cybersecurity and Infrastructure Security Agency.

''(3) With respect to such technologies, developing new capabilities for vulnerability discovery, management, and mitigation.

''(4) Assessing the security of software essential to national critical functions.

''(5) Supporting existing communities of interest, including by granting funds, in remediating vulnerabilities discovered within such technologies.

''(6) Utilizing findings to inform and support the future work of the Cybersecurity and Infrastructure Security Agency.

''(f) APPLICATION.—To be eligible for an award of a grant, contract, or cooperative agreement as a Critical Technology Security Center pursuant to subsection (a), a covered entity shall submit to the Secretary an application at such time, in such manner, and including such information as the Secretary may require.

''(g) PUBLIC REPORTING OF VULNERABILITIES.—The Undersecretary shall ensure that vulnerabilities identified by a Critical Technology Security Center are publicly reported through the National Vulnerability Database, as appropriate.

''(h) ADDITIONAL GUIDANCE.—The Under Secretary, in coordination with the Director, shall develop, and periodically update, guidance, including eligibility and any additional requirements, for how Critical Technology Security Centers may award funds to communities of interest to remediate vulnerabilities under subsection (e)(5).

''(i) BIANNUAL REPORTS.—Not later than one year after the date of the enactment of this section and every two years thereafter, the Under Secretary shall submit to the appropriate congressional committees a report that in-

cludes, with respect to each Critical Technology Security Center the following:

''(1) A summary of the work performed by each such center.

''(2) Information relating to the allocation of Federal funds at each such center.

''(3) A description of each vulnerability identified, including information relating to the corresponding software weakness.

''(4) An assessment of the criticality of each vulnerability identified pursuant to paragraph (3).

''(5) A list of critical technologies studied by each center, including an explanation by the Under Secretary for any deviations from the list of technologies provided by the Director before the distribution of funding to the center.

''(6) A list of tools, techniques, and procedures used by each such center.

''(j) CONSULTATION WITH RELEVANT AGENCIES.—In carrying out this section, the Under Secretary shall consult with the heads of other Federal agencies conducting cybersecurity research, including the following:

''(1) The National Institute of Standards and Technology.

''(2) The National Science Foundation.

''(3) Relevant agencies within the Department of Energy.

''(4) Relevant agencies within the Department of Defense.

''(k) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section—

''(1) $40,000,000 for fiscal year 2022;

''(2) $42,000,000 for fiscal year 2023;

''(3) $44,000,000 for fiscal year 2024;

''(4) $46,000,000 for fiscal year 2025; and

''(5) $49,000,000 for fiscal year 2026.

''(l) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate.

''(2) COVERED ENTITY.—The term 'covered entity' means a university or federally funded research and development center, including a national laboratory, or a consortia thereof.

''(3) CRITICAL TECHNOLOGY.—The term 'critical technology' means technology relating to a national critical function.

''(4) OPEN SOURCE SOFTWARE.—The term 'open source software' means software for which the human-readable source code is freely available for use, study, re-use, modification, enhancement, and redistribution by the users of such software.''.

(b) IDENTIFICATION OF CERTAIN TECHNOLOGY.—Paragraph (1) of section 2202(e) of the Homeland Security Act of 2002 (6 U.S.C. 603(e)) is amended by adding at the end the following new subparagraph:

''(S) To identify the technologies within the remits of the Critical Technology Security centers as described in section 322 that are vital to national critical functions.''.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 321 the following new item:

''Sec. 323. Critical Technology Security Centers.''.