AMENDMENT TO RULES COMM. PRINT 118–10
OFFERED BY MR. TORRES OF NEW YORK

Add at the end of subtitle C of title XVIII the following:

1 SEC. 1859. CRITICAL TECHNOLOGY SECURITY CENTERS.
2 (a) Critical Technology Security Centers.—
4 181 et seq.) is amended by adding at the end the following
5 new section:
6 “SEC. 324. CRITICAL TECHNOLOGY SECURITY CENTERS.
7 “(a) Establishment.—Not later than 180 days
8 after the date of the enactment of this section, the Sec-
9 retary, acting through the Under Secretary for Science
10 and Technology, and in coordination with the Director,
11 shall award grants, contracts, or cooperative agreements
12 to covered entities for the establishment of not fewer than
13 two cybersecurity-focused Critical Technology Security
14 Centers (in this section referred to as ‘Centers’) to eval-
15 uate and test the security of critical technology.
16 “(b) Evaluation and Testing.—In carrying out
17 the evaluation and testing of the security of critical tech-
18 nology pursuant to subsection (a), the Centers shall ad-
19 dress the following technologies:
“(1) The security of information and communications technology that underpins national critical functions related to communications.

“(2) The security of networked industrial equipment, such as connected programmable data logic controllers and supervisory control and data acquisition servers.

“(3) The security of open source software that underpins national critical functions.

“(4) The security of critical software used by the Federal Government.

“(c) ADDITION OR TERMINATION OF CENTERS.—

“(1) IN GENERAL.—The Under Secretary for Science and Technology may, in coordination with the Director, award or terminate grants, contracts, or cooperative agreements to covered entities for the establishment of additional or termination of existing Centers to evaluate and test the security of critical technologies.

“(2) LIMITATION.—The authority provided under paragraph (1) may be exercised except if such exercise would result in the operation at any time of fewer than two Centers.

“(d) SELECTION OF CRITICAL TECHNOLOGIES.—
“(1) IN GENERAL.—Before awarding a grant, contract, or cooperative agreement to a covered entity to establish a Center, the Under Secretary for Science and Technology shall coordinate with the Director, who shall provide the Under Secretary a list of critical technologies or guidance on such technologies that would be within the remit of any such Center.

“(2) EXPANSION AND MODIFICATION.—The Under Secretary for Science and Technology, in coordination with the Director, is authorized to expand or modify at any time the list of critical technologies or guidance on technologies referred to in paragraph (1) that is within the remit of a proposed or established Center.

“(e) RESPONSIBILITIES.—In carrying out the evaluation and testing of the security of critical technology pursuant to subsection (a), the Centers shall each have the following responsibilities:

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

“(2) Utilizing the coordinated vulnerability disclosure processes established under subsection (g) to report to the developers of such technologies and, as appropriate, to the Director, information relating to
vulnerabilities discovered and any information necessary to reproduce such vulnerabilities.

“(3) Developing new capabilities for improving the security of such technologies, including vulnerability discovery, management, mitigation, and remediation.

“(4) Assessing the security of software, firmware, and hardware that underpin national critical functions.

“(5) Supporting existing communities of interest, including through grant making, in mitigating and remediating vulnerabilities discovered within such technologies.

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

“(f) Risk Based Evaluations.—Unless otherwise directed pursuant to guidance issued by the Under Secretary for Science and Technology or Director under subsection (d), to the greatest extent practicable activities carried out pursuant to the responsibilities specified in subsection (e) shall leverage risk-based evaluations to focus on activities that have the greatest effect on the security of the critical technologies within each Center’s remit, such as the following:
“(1) Developing capabilities that can detect or
eliminate entire classes of vulnerabilities.

“(2) Testing for vulnerabilities in the most
widely used critical technologies, or vulnerabilities
that affect many such critical technologies.

“(g) COORDINATED VULNERABILITY DISCLOSURE
PROCESSES.—Each Center shall establish, in coordination
with the Director, coordinated vulnerability disclosure
processes regarding the disclosure of vulnerabilities that—

“(1) are adhered to when a vulnerability is dis-
covered or disclosed by each such Center, consistent
with international standards and coordinated vulner-
ability disclosure best practices; and

“(2) are published on the website of each such
Center.

“(h) APPLICATION.—To be eligible for an award of
a grant, contract, or cooperative agreement as a Center,
a covered entity shall submit to the Secretary an applica-
tion at such time, in such manner, and including such in-
formation as the Secretary may require.

“(i) PUBLIC REPORTING OF VULNERABILITIES.—
The Under Secretary for Science and Technology shall en-
sure that vulnerabilities discovered by a Center are re-
ported to the National Vulnerability Database of the Na-
tional Institute of Standards and Technology, as appro-
priate and using the coordinated vulnerability disclosure
processes established under subsection (g).

“(j) ADDITIONAL GUIDANCE.—The Under Secretary
for Science and Technology, in coordination with the Di-
rector, shall develop, and periodically update, guidance, in-
cluding eligibility and any additional requirements, rela-
ting to how Centers may award grants to communities of
interest pursuant to subsection (e)(5) to mitigate and re-
mediate vulnerabilities and take other actions under such
subsection and subsection (k).

“(k) OPEN SOURCE SOFTWARE SECURITY
GRANTS.—

“(1) IN GENERAL.—Any Center addressing
open source software security may, in consultation
with the Under Secretary for Science and Tech-
nology and Director, award grants to individual open
source software developers and maintainers, non-
profit organizations, and other non-Federal entities
as determined appropriate by any such Center, to
fund improvements in the security of the open
source software ecosystem.

“(2) IMPROVEMENTS.—A grant awarded under
paragraph (1) may include improvements such as
the following:

“(A) Security audits.
“(B) Funding for developers to patch vulnerabilities.

“(C) Addressing code, infrastructure, and structural weaknesses, including rewrites of open source software components in memory-safe programming languages.

“(D) Research and tools to assess and improve the overall security of the open source software ecosystem, such as improved software fault isolation techniques.

“(E) Training and other tools to aid open source software developers in the secure development of open source software, including secure coding practices and secure systems architecture.

“(3) PRIORITY.—In awarding grants under paragraph (1), a Center shall prioritize, to the greatest extent practicable, the following:

“(A) Where applicable, open source software components identified in guidance from the Director, or if no such guidance is so provided, utilizing the risk-based evaluation described in subsection (f).
“(B) Activities that most promote the long-term security of the open source software ecosystem.

“(l) Biennial Reports to Under Secretary.—Not later than one year after the date of the enactment of this section and every two years thereafter, each Center shall submit to the Under Secretary for Science and Technology, Director, and the appropriate congressional committees a report that includes the following:

“(1) A summary of the work performed by such Center.

“(2) Information relating to the allocation of Federal funds at such Center.

“(3) A list of critical technologies studied by such Center.

“(4) A description of each vulnerability that has been publicly disclosed pursuant to subsection (g), including information relating to the corresponding software weakness.

“(5) An assessment of the criticality of each such vulnerability.

“(6) An overview of the methodologies used by such Center, such as tactics, techniques, and procedures.
“(7) A description of such Center’s development of capabilities for vulnerability discovery, management, and mitigation.

“(8) A summary of such Center’s support to existing communities of interest, including an accounting of dispersed grant funds.

“(9) For such Center, if applicable, a summary of any grants awarded during the period covered by the report that includes the following:

“(A) An identification of the entity to which each such grant was awarded.

“(B) The amount of each such grant.

“(C) The purpose of each such grant.

“(D) The expected impact of each such grant.

“(10) The coordinated vulnerability disclosure processes established by such Center.

“(m) REPORTS TO CONGRESS.—Upon receiving the reports required under subsection (l), the Under Secretary for Science and Technology shall submit to the appropriate congressional committees a summary of such reports, and, where applicable, an explanation for any deviations in the list of critical technologies studied by a Center from the list of critical technologies or guidance relat-
ing to such technologies provided by the Director pursuant
to subsection (d).

“(n) CONSULTATION WITH RELEVANT AGENCIES.—
In carrying out this section, the Under Secretary shall consult with the heads of other Federal agencies con-
ducting cybersecurity research, including the following:

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

“(2) The National Science Foundation.

“(3) Relevant agencies of the Department of Energy.

“(4) Relevant agencies of the Department of Defense.

“(o) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section the following:

“(1) $42,000,000 for fiscal year 2024.

“(2) $44,000,000 for fiscal year 2025.

“(3) $46,000,000 for fiscal year 2026.

“(4) $49,000,000 for fiscal year 2027.

“(5) $52,000,000 for fiscal year 2028.

“(p) DEFINITIONS.—In this section:

“(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional commit-
mittees’ 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 that underpins one or more national critical functions.

“(4) CRITICAL SOFTWARE.—The term ‘critical software’ has the meaning given such term by the National Institute of Standards and Technology pursuant to Executive Order 14028 or any successor provision.

“(5) OPEN SOURCE SOFTWARE.—The term ‘open source software’ means software for which the human-readable source code is made available to the public for use, study, re-use, modification, enhancement, and redistribution.

“(6) DIRECTOR.—The term ‘Director’ means the Director of the Cybersecurity and Infrastructure Security Agency.”.
(b) IDENTIFICATION OF CERTAIN TECHNOLOGY.—

Paragraph (1) of section 2202(e) of the Homeland Security Act of 2002 (6 U.S.C. 652(e)) is amended by adding at the end the following new subparagraph:

“(S) To identify the critical technologies (as such term is defined in section 324) or develop guidance relating to such technologies within the remits of the Critical Technology Security Centers as described in such section.”.

(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 323 the following new item:

“Sec. 324. Critical Technology Security Centers.”.