AMENDMENT TO H.R. 8462

OFFERED BY MR. SUBRAMANYAM OF VIRGINIA

Insert after section 24 the following:

SEC. 25. REPORTS ON MITIGATING THE CYBERSECURITY AND NATIONAL SECURITY RISKS POSED BY CERTAIN QUANTUM COMPUTERS.

(a) INITIAL REPORT.—Not later than one year after the date of the enactment of this Act, the Subcommittee on the Economic and Security Implications of Quantum Information Science established under section 105 of the National Quantum Initiative Act (15 U.S.C. 8814a) shall carry out the following:

(1) Conduct an assessment of each of the following:

(A) The capabilities and progress of the United States, relative to other countries, with respect to the following:

(i) Developing a cryptographically-relevant quantum computer.

(ii) Adopting security and preparedness measures, including post-quantum cryptography, to mitigate the cybersecurity

and national security risks posed by such computer.

(B) The progress of private sector entities and public sector entities in the United States toward adopting such measures, including the progress toward implementing the guidance under section 4 of the Quantum Computing Cybersecurity Preparedness Act (6 U.S.C. 1526).

(2) Identify the sectors of the economy most vulnerable to such risks.

(3) Based upon such assessments and such identification, develop a plan to mitigate such risks, including by carrying out the following:

(A) Facilitating collaboration between agencies and departments of the Federal Government.

(B) Facilitating the exchange of information between such private sector entities and public sector entities.

(C) Forming partnerships between the Federal Government and such private sector entities.

(D) Identifying such measures that such private sector entities and public sector entities may adopt.

(E) Supporting such exchange and the adoption of such measures, including by identifying actions, including piloting projects, providing technical assistance, and publishing cyber hygiene guidance for such private sector entities, that such agencies and departments may carry out to support such exchange and adoption.

(4) Develop guidelines for determining whether a quantum computer is a cryptographically-relevant quantum computer.

(5) Submit to the appropriate committees of Congress a report in classified or unclassified form, as appropriate, that includes information relating to the following:

(A) The assessments conducted under paragraph (1).

(B) The sectors identified under paragraph (2).

(C) The plan developed under paragraph (3).

(D) The guidelines developed under paragraph (4).

(E) Recommendations for the following:

(i) A timetable to implement such plan.

(ii) Policies to implement such plan that require legislation.

(iii) Policies to implement such plan that do not require legislation.

(b) SUBSEQUENT REPORTS.—Not later than one year after the report under subsection (a) is submitted and annually thereafter for four years, the Subcommittee referred to in such subsection shall submit to Congress a report in classified or unclassified form, as appropriate, that includes information relating to the progress of private sector entities and public sector entities in the United States toward adopting the measures described in such subsection.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' has the meaning given such term in section 2 of the National Quantum Initiative Act (15 U.S.C. 8801).

(2) CLASSICAL COMPUTER; POST-QUANTUM CRYPTOGRAPHY; QUANTUM COMPUTER.—The terms ''classical computer'', ''post-quantum cryptography'', and ''quantum computer'' have the meanings given

such terms in section 3 of the Quantum Computing Cybersecurity Preparedness Act (6 U.S.C. 1526 note).

(3) CRYPTOGRAPHICALLY-RELEVANT QUANTUM COMPUTER.—The term ''cryptographically-relevant quantum computer'' means a quantum computer with the ability to compromise a cryptographic system that a classical computer is unable to compromise.