AMENDMENT TO THE AMENDMENT IN THE
NATURE OF A SUBSTITUTE TO H.R. 6213
OFFERED BY MR. JACKSON OF NORTH CAROLINA
And Ms. Tenney of New York

Page 24, beginning line 7, insert the following:

(C) by amending paragraph (3) to read as follows:

“(3) shall carry out research to facilitate the development and standardization of quantum cryptography, post-quantum cryptography (as such term is defined in section 3 of the Quantum Computing Cybersecurity Preparedness Act (6 U.S.C. 1526 note; Public Law 117–260)), and practices to replace cryptographic keys or algorithms with minimal disruption to current applications and systems;”.

Page 29, beginning line 13, insert the following:

“(d) POST QUANTUM CRYPTOGRAPHY DEPLOYMENT.—

“(1) IN GENERAL.—The Director of the National Institute of Standards and Technology, in consultation with the Secretary of Homeland Security, the heads of Sector Risk Management Agencies (as such term is defined in section 2200 of the
Homeland Security Act of 2002 (6 U.S.C. 650)), and private sector entities, as appropriate, shall pro-
mote the voluntary development, adoption, and de-
ployment of standards relating to post-quantum
cryptography (as such term is defined in section 3
of the Quantum Computing Cybersecurity Prepared-
ness Act (6 U.S.C. 1526 note; Public Law 117–
260)), including by—

“(A) disseminating and making publicly
available guidance and resources to help organi-
izations adopt and deploy standards relating to
post-quantum cryptography and minimize dis-
ruptions to current applications and systems
caused by cryptographic updates;

“(B) providing technical assistance, as
practicable, to entities that are at high risk of
quantum cryptoanalytic attacks, such as enti-
ties determined to be critical infrastructure (as
such term is defined in section 1016(e) of Pub-
lic Law 107–56 (42 U.S.C. 5195e(e))) or dig-
ital infrastructure providers; and

“(C) conducting such other activities as
determined necessary by the Director to pro-
mote the development, adoption, and deploy-
ment across the United States of standards relating to post-quantum cryptography.

“(2) GRANT PROGRAM.—

“(A) IN GENERAL.—Subject to the availability of appropriations and after the date on which the Director of National Institute of Standards and Technology has issued standards relating to post-quantum cryptography, the Director may establish a program to identify and provide technical assistance through the award of grants to entities that are at high risk of quantum cryptoanalytic attacks, including by granting funds for the adoption of such standards and the remediation of quantum-related vulnerabilities.

“(B) USE OF FUNDS.—Grants awarded to entities under this paragraph may be used to cover reasonable costs, up to a specified amount established by the Director of the National Institute of Standards and Technology, for activities to adopt standards relating to post-quantum cryptographic and remediate quantum-related vulnerabilities.

“(C) GUIDANCE.—The Director of the National Institute of Standards and Technology
may develop, and periodically update, guidance, including relating to eligibility, application disclosure requirements, grant amount and duration, and any additional requirements regarding the award of grants under this paragraph.

“(D) CONSULTATION.—If the program described in this paragraph is established, the Director of the National Institute of Standards and Technology shall consult with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, the heads of other Sector Risk Management Agencies, and appropriate representatives of private sector entities, including non-profit organizations, to share information regarding the grant program under this paragraph and guidance developed and updated under subparagraph (C).”.

Page 75, beginning line 14, insert the following:

19 SEC. 22. NATIONAL SCIENCE FOUNDATION CRYPTOGRAPHY RESEARCH.

Subsection (a)(1)(A) of section 4 of the Cyber Security Research and Development Act (15 U.S.C. 7403) is amended by inserting “, including post-quantum cryptography (as such term is defined in section 3 of the Quan-