AMENDMENT TO RULES COMMITTEE PRINT 118–36

OFFERED BY MR. HIMES OF CONNECTICUT

At the end of title XVII, add the following:

Subtitle D—Prohibition on Use by the Department of Defense of Commercial Spyware That Poses Risks to National Security.

SEC. 1761. FINDINGS.

Congress finds the following:

(1) Technology is central to the future of our national security, economy, and democracy. The United States has fundamental national security and foreign policy interests in—

(A) ensuring that technology is developed, deployed, and governed in accordance with universal human rights, the rule of law, and appropriate legal authorization, safeguards, and oversight, such that it supports, and does not undermine, democracy, civil rights and civil liberties, and public safety; and

(B) mitigating, to the greatest extent possible, the risk emerging technologies may pose to Department of Defense institutions, personnel, information, and information systems.

(2) To advance these interests, the United States supports the development of an international technology ecosystem that protects the integrity of international standards development, enables and promotes the free flow of data and ideas with trust, protects our security, privacy, and human rights, and enhances our economic competitiveness. The growing exploitation of Americans' sensitive data and improper use of surveillance technology, including commercial spyware, threatens the development of this ecosystem. Foreign governments and persons have deployed commercial spyware against Department of Defense institutions, personnel, information, and information systems, presenting significant counterintelligence and security risks to the Department of Defense. Foreign governments and persons have also used commercial spyware for improper purposes, such as to target and intimidate perceived opponents, curb dissent, limit freedoms of expression, peaceful assembly, or association, enable other human rights abuses or suppression of civil liberties,

and track or target United States persons without proper legal authorization, safeguards, or oversight.

(3) The United States has a fundamental national security and foreign policy interest in countering and preventing the proliferation of commercial spyware that has been or risks being misused for such purposes, in light of the core interests of the United States in protecting Department of Defense personnel and United States citizens around the world, upholding and advancing democracy, promoting respect for human rights, and defending activists, dissidents, and journalists against threats to their freedom and dignity. To advance these interests and promote responsible use of commercial spyware, the United States must establish robust protections and procedures to ensure that any Department of Defense use of commercial spyware helps protect its information systems and intelligence and law enforcement activities against significant counterintelligence or security risks, aligns with its core interests in promoting democracy and democratic values around the world, and ensures that the Department of Defense does not contribute, directly or indirectly, to the proliferation of commer-

cial spyware that has been misused by foreign governments or facilitate such misuse.

(4) It is the policy of the Department of Defense that it shall not make operational use of commercial spyware that poses significant counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person. In furtherance of the national security and foreign policy interests of the United States, this subtitle accordingly directs steps to implement that policy and protect the safety and security of Department of Defense institutions, personnel, information, and information systems, discourage the improper use of commercial spyware, and encourage the development and implementation of responsible norms regarding the use of commercial spyware that are consistent with respect for the rule of law, human rights, and democratic norms and values.

SEC. 1762. PROHIBITION ON OPERATIONAL USE.

(a) USE OF COMMERCIAL SPYWARE.—The Department of Defense shall not make operational use of commercial spyware where they determine, based on credible information, that such use poses significant counterintelligence or security risks to the Department of Defense or

that the commercial spyware poses significant risks of improper use by a foreign government or foreign person. For the purposes of this use prohibition:

(1) Commercial spyware may pose counterintelligence or security risks to the Department of Defense when—

(A) a foreign government or foreign person has used or acquired the commercial spyware to gain or attempt to gain access to Department of Defense computers or the computers of Department of Defense personnel without authorization from the Department of Defense; or

(B) the commercial spyware was or is furnished by an entity that—

(i) maintains, transfers, or uses data obtained from the commercial spyware without authorization from the licensed end-user or the Department of Defense;

(ii) has disclosed or intends to disclose non-public Department of Defense information or non-public information about the activities of the Department of Defense without authorization from the Department of Defense; or

(iii) is under the direct or effective control of a foreign government or foreign person engaged in intelligence activities, including surveillance or espionage, directed against the United States.

(2) Commercial spyware may pose risks of improper use by a foreign government or foreign person when—

(A) the commercial spyware, or other commercial spyware furnished by the same vendor, has been used by a foreign government or foreign person—

(i) to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons, curb dissent or political opposition, otherwise limit freedoms of expression, peaceful assembly, or association, or enable other forms of human rights abuses or suppression of civil liberties; or

(ii) to monitor a United States person, without such person's consent, in order to facilitate the tracking or targeting

of the person without proper legal authorization, safeguards, and oversight; or

(B) the commercial spyware was furnished by an entity that provides commercial spyware to governments for which there are credible reports in the annual country reports on human rights practices of the Department of State that they engage in systematic acts of political repression, including arbitrary arrest or detention, torture, extrajudicial or politically motivated killing, or other gross violations of human rights, consistent with any findings by the Department of State pursuant to section 5502 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81) or other similar findings.

(3) In determining whether the operational use of commercial spyware poses significant counterintelligence or security risks to the Department of Defense or poses significant risks of improper use by a foreign government or foreign person, such that operational use should be prohibited, the Secretary of Defense shall consider, among other relevant considerations, whether the entity furnishing the commercial spyware knew or reasonably should have

known that the spyware posed risks described in paragraphs (1) and (2), and whether the entity has taken appropriate measures to remove such risks, such as canceling relevant licensing agreements or contracts that present such risks, taking other verifiable action to prevent continuing uses that present such risks, or cooperating in Department of Defense efforts to counter improper use of the spyware.

(b) REQUESTS OF THIRD PARTIES.—The Department of Defense shall not request or directly enable a third party to make operational use of commercial spyware where the Secretary of Defense has determined that such use poses significant counterintelligence or security risks to the Department of Defense or that the commercial spyware poses significant risks of improper use by a foreign government or foreign person, as described in subsection (a). For purposes of this subsection, the term ''operational use'' includes such indirect use.

(c) INTELLIGENCE ASSESSMENT.—The Director of National Intelligence (hereafter referred to as the ''DNI'') shall, within 90 days of the date of enactment of this section, and on a semiannual basis thereafter, issue a classified intelligence assessment that integrates relevant information (including intelligence, open source, financial,

sanctions-related, and export controls-related information) on foreign commercial spyware or foreign government or foreign person use of commercial spyware relevant to the factors set forth in subsection (a). The intelligence assessment shall include the report and assessment required by section 1102A(b) of the National Security Act of 1947 (50 U.S.C. 3232a). In order to facilitate the production of the intelligence assessment, the Secretary of Defense shall, on an ongoing basis, provide the DNI all new credible information obtained by the Department of Defense on foreign commercial spyware vendors or foreign government or foreign person use of commercial spyware relevant to the factors set forth in subsection (a). Such information shall include intelligence, open source, financial, sanctions-related, export controls-related, and due diligence information, as well as information relevant to the development of the list of covered contractors developed or maintained pursuant to section 5502 of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117–81) or other similar information.

(d) CERTIFICATION OF DETERMINATION TO USE COMMERCIAL SPYWARE.—For any commercial spyware intended by the Department of Defense for operational use, the Secretary of Defense shall certify the determination that the commercial spyware does not pose significant

counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person based on the factors set forth in subsection (a).

(e) REVIEW OF EXISTING USE OF COMMERCIAL SPYWARE.—Within 90 days of the issuance of the intelligence assessment described in subsection (c), the Secretary of Defense shall review all existing operational uses of commercial spyware and discontinue, as soon as the Secretary of Defense determines is reasonably possible without compromising ongoing operations, operational use of any commercial spyware that the Secretary of Defense determines poses significant counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person, pursuant to subsection (a).

(f) DEVELOPMENT OF INTERNAL CONTROLS AND OVERSIGHT PROCEDURES.—Within 180 days of the date of enactment of this section, if the Department of Defense makes operational use of commercial spyware, the Department of Defense shall develop appropriate internal controls and oversight procedures for conducting determinations under subsection (a), as appropriate and consistent with applicable law.

(g) DETERMINATIONS BASED ON LATER OBTAINED INFORMATION.—At any time after procuring commercial spyware for operational use, if the Department of Defense obtains relevant information with respect to the factors set forth in subsection (a), the Department of Defense shall determine whether the commercial spyware poses significant counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person, and, if so, shall terminate such operational use as soon as the Secretary of Defense determines is reasonably possible without compromising ongoing operations, and shall notify the DNI.

(h) FEDERAL ACQUISITION SECURITY COUNCIL.—The Federal Acquisition Security Council shall consider the intelligence assessment described in subsection (c) in evaluating whether commercial spyware poses a supply chain risk, as appropriate and consistent with applicable law, including part 201 of title 41, Code of Federal Regulations, and section 1323 of title 41, United States Code.

(i) APPLICABILITY TO TESTING, RESEARCH, AND RELATED MATTERS.—The prohibitions contained in this section shall not apply to the use of commercial spyware for purposes of testing, research, analysis, cybersecurity, or the development of countermeasures for counterintelligence or security risks, or for purposes of a criminal in-

vestigation arising out of the criminal sale or use of the spyware.

(j) WAIVERS.—The Secretary of Defense may issue a waiver, for a period not to exceed 1 year, of an operational use prohibition determined pursuant to subsection (a) if the Secretary of Defense determines that such waiver is necessary due to extraordinary circumstances and that no feasible alternative is available to address such circumstances. The Secretary of Defense may, at any time, revoke any waiver previously granted. Within 72 hours of making a determination to issue or revoke a waiver pursuant to this subsection, the Secretary of Defense shall notify the President of the determination, including the justification for the determination. The Secretary of Defense shall provide this information concurrently to the DNI.

SEC. 1763. APPLICATION TO PROCUREMENT.

If the Department of Defense is seeking to procure commercial spyware for any purpose other than for a criminal investigation arising out of the criminal sale or use of the spyware, the Department of Defense shall, prior to making such procurement and consistent with its existing statutory and regulatory authorities—

(1) review the intelligence assessment issued by the DNI pursuant to section 1762(c);

(2) request from the DNI any additional information regarding the commercial spyware that is relevant to the factors set forth in section 1762(a);

(3) consider the factors set forth in section 1762(a) in light of the information provided by the DNI; and

(4) consider whether any entity furnishing the commercial spyware being considered for procurement has implemented reasonable due diligence procedures and standards (such as the industry-wide norms reflected in relevant Department of State guidance on business and human rights and on transactions linked to foreign government end-users for products or services with surveillance capabilities) and controls that would enable the entity to identify and prevent uses of the commercial spyware that pose significant counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person.

SEC. 1764. REPORTING REQUIREMENTS.

(a) REPORT ON PROCUREMENT.—If the Secretary of Defense has procured commercial spyware, upon completing the review described in section 1762(e), the Secretary of Defense shall submit to the President a report

describing the review's findings. If the review identifies any existing operational use of commercial spyware the report shall include—

(1) a description of such existing operational use;

(2) a determination of whether the commercial spyware poses significant counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person, along with key elements of the underlying analysis, pursuant to section 1762(a); and

(3) in the event the Secretary of Defense determines that the commercial spyware poses significant risks pursuant to section 1762(a), what steps have been taken to terminate its operational use.

(b) NOTIFICATION FOR PROCUREMENT.—Within 45 days of a Department of Defense's procurement of any commercial spyware for any use described in section 1762(i) except for use in a criminal investigation arising out of the criminal sale or use of the spyware, the Secretary of Defense shall notify the President of such procurement and shall include in the notification a description of the purpose and authorized uses of the commercial spyware.

(c) ANNUAL REPORT ON PROCUREMENT.—Within 1 year of the date of enactment this section, and on an annual basis thereafter, if the Secretary of Defense has procured commercial spyware for operational use, the Secretary of Defense shall provide the President a report that identifies—

(1) any existing operational use of commercial spyware and the reasons why it does not pose significant counterintelligence or security risks to the Department of Defense or significant risks of improper use by a foreign government or foreign person, pursuant to section 1762(a);

(2) any operational use of commercial spyware that was terminated during the preceding year because it was determined to pose significant risks pursuant to section 1762(a), the circumstances under which this determination was made, and the steps taken to terminate such use; and

(3) any purchases made of commercial spyware, and whether they were made for operational use, during the preceding year.

SEC. 1765. GENERAL PROVISIONS.

(a) AUTHORITY; FUNCTIONS.—Nothing in this subtitle shall be construed to impair or otherwise affect—

(1) the authority granted by any other provision of law to the Department of Defense, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) REMEDIES.—Nothing in this subtitle shall be construed to limit the use of any remedies available to the Secretary of Defense or any other official of the Department of Defense.

(c) NO NEW RIGHT OR BENEFIT.—This subtitle is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

SEC. 1766. DEFINITIONS.

For purposes of this subtitle:

(1) The term ''commercial spyware'' means any end-to-end software suite that is furnished for commercial purposes, either directly or indirectly through a third party or subsidiary, that provides the user of the software suite the capability to gain remote access to a computer, without the consent of

the user, administrator, or owner of the computer, in order to—

(A) access, collect, exploit, extract, intercept, retrieve, or transmit content, including information stored on or transmitted through a computer connected to the Internet;

(B) record the computer's audio calls or video calls or use the computer to record audio or video; or

(C) track the location of the computer.

(2) The term ''computer'' shall have the same meaning as it has in section 1030(e)(1) of title 18, United States Code.

(3) The term ''entity'' means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

(4) The term ''foreign government'' means any national, state, provincial, or other governing authority, any political party, or any official of any governing authority or political party, in each case of a country other than the United States.

(5) The term ''foreign person'' means a person that is not a United States person.

(6) The term ''furnish'', when used in connection with commercial spyware, means to develop,

maintain, own, operate, manufacture, market, sell, resell, broker, lease, license, repackage, rebrand, or otherwise make available commercial spyware.

(7) The term ''operational use''—

(A) means use to gain remote access to a computer, without the consent of the user, administrator, or owner of the computer, in order to—

(i) access, collect, exploit, extract, intercept, retrieve, or transmit the computer's content, including information stored on or transmitted through a computer connected to the Internet;

(ii) record the computer's audio calls or video calls or use the computer to otherwise record audio or video; or

(iii) track the location of the computer; and

(B) does not include those uses described in section 1762(i).

(8) The term ''person'' means an individual or entity.

(9) The term ''remote access'' when used in connection with commercial spyware, means access to a computer, the computer's content, or the com-

puter's components by using an external network (including the Internet) when the computer is not in the physical possession of the actor seeking access to that computer.

(10) The term ''United States entity'' means any entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches).

(11) The term ''United States person'' shall have the same meaning as it has in Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended.

☒