AMENDMENT NO.________ Calendar No.______

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—119th Cong., 2d Sess.

S. 4570

To incentivize, streamline, and sustain United States foreign government partner procurement of United States-origin cyber and digital technologies.

Referred to the Committee on ____________________ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mrs. SHAHEEN (for herself and Mr. RICKETTS)

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "U.S. Technology Procurement and Access to Trusted Hardware Act" or the "U.S. Tech PATH Act".

SEC. 2. DEFINITIONS.

In this Act:

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

(A) the Committee on Foreign Relations and the Committee on Commerce, Science, and Transportation of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Energy and Commerce of the House of Representatives.

(2) FOREIGN COUNTRY OF CONCERN.—The term ''foreign country of concern'' has the meaning given the term ''covered nation'' in section 4872(f) of title 10, United States Code.

(3) FOREIGN GOVERNMENT PARTNER.—The term ''foreign government partner'' includes international organizations.

(4) INTERNATIONAL ORGANIZATIONS.—The term ''international organizations'' has the meaning given the term in section 1 of the International Organizations Immunities Act (22 U.S.C. 288).

(5) TRUSTED CYBER AND DIGITAL TECHNOLOGIES.—The term ''trusted cyber and digital technologies'' means technologies, including equipment, services, hardware, or software used in information and communications technology networks, for which the Secretary of State, in coordination with the Secretary of Commerce, has determined—

(A) the provider, supplier, or manufacturer is not owned by, controlled by, or subject to the influence of a foreign country of concern; and

(B) do not pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(6) PAX SILICA INITIATIVE.—The term ''Pax Silica *initiative*'' refers to the Department of State-led diplomatic, economic security, and supply chain initiative, announced on December 11, 2025, to strengthen cooperation among the United States, allied countries, partner countries, industry, and other relevant stakeholders for the purpose of developing and securing trusted supply chains and infrastructure necessary for artificial intelligence, semiconductors, advanced manufacturing, and other technologies determined by the Secretary of State to be essential to United States national security, economic security, and technological competitiveness.

SEC. 3. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) foreign government partners are increasingly turning towards strategic competitors like the People's Republic of China to procure cyber and dig-

ital technologies due to their low-cost, acceptable efficacy, ease and speed of acquisition, and support for associated training and maintenance;

(2) foreign government partner procurement of cyber and digital technologies from suppliers aligned with strategic competitors of the United States poses significant and distinct risks, including—

(A) supply chain vulnerabilities created by dependence on strategic competitors whose governments may compel access to data, networks, or systems, undermining the cybersecurity and strategic autonomy of the procuring government;

(B) the erosion of interoperability and alignment with United States cybersecurity frameworks, standards, and best practices, reducing the ability of foreign government partners to operate securely alongside United States systems and those of United States allies; and

(C) the adoption of digital governance practices that are inconsistent with United States economic and national security interests;

(3) United States foreign government partners consistently signal strong demand for trusted cyber

and digital technologies from United States suppliers;

(4) United States initiatives such as Pax Silica should facilitate technology procurements by building enduring technology partnerships between foreign government partners and United States suppliers, including by—

(A) assisting foreign government partners in navigating regulatory, logistical, and technical hurdles to trusted cyber and digital technology procurement;

(B) providing foreign government partners with strategic direction from the United States Government;

(C) incorporating foreign government partner needs into program development from the outset; and

(D) maintaining long-term engagement with foreign government partners throughout the procurement cycle of trusted cyber and digital technologies; and

(5) as the United States seeks to maintain its global competitive edge in critical and emerging technologies, including advanced cybersecurity, artificial intelligence, advanced telecommunications, and

robotics, it is in the interest of the United States Government to establish policies and procedures that streamline foreign government partners' ability to procure trusted and reliable technologies from the United States and United States allies and partners.

SEC. 4. UNITED STATES TECHNOLOGY PROCUREMENT PROGRAM.

(a) ESTABLISHMENT.—There is established in the Department of State the United States Cyber and Digital Technology Procurement Program (referred to in this Act as the ''Program''), which shall be administered by the Bureau for Cyberspace and Digital Policy, and which may support Pax Silica and other related initiatives. To the maximum extent practicable, the Program shall seek to serve as a demand-driven mechanism in response to cyber and digital technology needs as determined by the participating foreign government partner.

(b) PURPOSES.—The purposes of the Program shall include the following:

(1) To streamline foreign government partner procurement of trusted cyber and digital technologies, including commercial off-the-shelf technologies, consistent with United States export control laws, including cybersecurity standards appropriate to relevant policy goals of the United States.

(2) To establish long-term cyber and digital technology procurement pipelines with United States providers, including after the termination of the Program.

(3) To identify the appropriate United States Government financing mechanisms to address challenges associated with affordability of trusted cyber and digital technologies.

(4) To provide a comprehensive package to foreign government partners, with the support of and in coordination with United States industry technical experts, as appropriate, to navigate trusted cyber and digital technology procurement requirements, to understand technical and system complexity, to assess absorptive capacity, and to identify foreign government partner-specific logistical and export control challenges, including by—

(A) designing and implementing procurement, deployment, and technical knowledge transfer that enable the participating foreign government partner to modernize and secure systems;

(B) providing clear guidelines for United States and trusted foreign supplier entry and eligibility;

(C) conducting assessments related to the participating foreign government partner's workforce or technological requirements, including any gaps in absorptive capacity, including—

(i) feasibility studies to identify, design, and implement the deployment of trusted cyber and digital technology solutions; and

(ii) sustainability assessments to determine the participating foreign government partner's ability to procure and invest in trusted cyber and digital technologies, including the ability to sustain such investments in the long-term;

(D) providing capacity building to ensure that the participating foreign government partner obtains the relevant skills for requirements identification and assessment, integration of United States procurements into existing operating environments, research and procurement, logistics, deployment, and configuration to ensure a long-term arrangement with United States suppliers; and

(E) assisting the participating foreign government partner in developing a long-term strategy to procure and budget for trusted cyber and digital technology procurements, including beyond the end of the Program's lifecycle.

(5) To assess the risks and tradeoffs of foreign government partners adopting cyber and digital technologies from foreign countries of concern and prioritize foreign government partners for outreach efforts based on that risk assessment.

(c) COVERED CYBER AND DIGITAL TECHNOLOGIES.—In implementing the Program, the Secretary of State shall, in coordination with the participating foreign government partner and United States industry technical experts, as appropriate, prioritize the following trusted cyber and digital technologies, as well as any other trusted cyber and digital technologies designated by the Secretary pursuant to subsection (d):

(1) Software and its associated subscriptions and licensing, including—

(A) operating systems;

(B) enterprise management software;

(C) cloud-based storage solutions and compute access;

(D) industrial control and automation software, including Supervisory Control and Data

Acquisition (SCADA), distributed control systems (DCS), and programmable logic controller (PLC) programming environments;

(E) digital twin, simulation, and modeling software; and

(F) cloud and edge orchestration platforms for robotic and operational technology (OT) device management.

(2) Hardware, including—

(A) processors;

(B) human-machine interfaces (HMIs) and operator consoles;

(C) networking equipment, including switches, routers, and gateways;

(D) industrial networking equipment;

(E) biotechnology equipment, including genomic sequencers and related hardware; and

(F) other related technologies.

(3) Cybersecurity products, including—

(A) firewalls;

(B) intrusion detection and prevention systems;

(C) Security Information and Event Management (SIEM) systems;

(D) threat intelligence and monitoring systems;

(E) endpoint detection systems;

(F) Security Operations Centers (SOC);

(G) secure authentication systems; and

(H) cybersecurity training and consulting services.

(4) Telecommunications equipment, including—

(A) subsea fiber-optic cable and associated equipment;

(B) cellular equipment, including open radio access network (ORAN) equipment;

(C) satellite-enabling infrastructure; and

(D) broadband infrastructure, including fiber optic network equipment.

(5) Equipment and related products to enable the adoption of artificial intelligence (AI) solutions, including—

(A) compute;

(B) storage;

(C) memory;

(D) models, including both closed- and open-weight models;

(E) AI model licenses;

(F) edge AI capabilities, including next-generation smartphone technology and relevant mobile operating systems; and

(G) AI model applications.

(d) ANNUAL REVIEW OF COVERED CYBER AND DIGITAL TECHNOLOGIES.—The Secretary of State shall conduct an annual assessment to identify the inclusion or removal of technologies under subsection (c) based on the national security risk to the United States of a foreign country of concern gaining significant market share of such technology within a foreign government partner country.

(e) RISK MITIGATION REQUIREMENTS.—The Secretary shall—

(1) before approving a partnership under the Program—

(A) conduct, and submit to the appropriate congressional committees, an initial assessment of cyber and digital technology misuse and diversion risks, including—

(i) the foreign government partner's export control enforcement capacity;

(ii) the foreign government partner's history of technology transfer to foreign countries of concern, including permitting remote access to technology; and

(iii) investments by foreign countries of concern in the foreign government partner's critical sectors;

(B) establish monitoring and mitigation requirements proportional to the risk assessed under paragraph (1);

(C) include end-use monitoring provisions in all Program agreements; and

(D) coordinate with the intelligence community and the Department of Defense regarding counterintelligence and national security risks; and

(2) on an annual basis for the duration of a partnership under the Program, update and submit to the appropriate congressional committees the assessment required by paragraph (1) in order to continually assess the conditions described in clauses (i), (ii), and (iii) of paragraph (1)(A), including any improvements in such conditions.

(f) FOREIGN GOVERNMENT PARTNER CONTRIBUTION.—For any partnership with a foreign government partner under the Program, the Secretary shall, to the maximum extent practicable, seek to ensure cost-sharing with the foreign government partner to facilitate the foreign government partner's long-term buy-in and sustained procurements of trusted cyber and digital technologies.

(g) ADDITIONAL INTERAGENCY COORDINATION.—In implementing the Program, to address challenges associated with affordability, financing, technical evaluations, procurement requirements, and long-term capacity building, the Secretary of State shall, on a case-by-case basis, coordinate, as appropriate, with the relevant Federal agencies, including the Department of Commerce, the United States International Development Finance Cooperation, and the United States Trade and Development Agency.

(h) USE OF FUNDS.—Funds made available to carry out the Program shall be used—

(1) to provide assistance or financing—

(A) to foreign government partner civilian government agencies; or

(B) to law enforcement or military agencies, only if such entities are the owners and operators of the foreign government partner's civilian critical infrastructure; and

(2) to develop blended finance mechanisms, co-developed with the participating foreign government partner, that partners with fund managers, project developers, third-party investors, infrastructure pro-

viders, and other private partners to advance the objections outlined in subsection (b).

(i) PARTNER DISQUALIFICATION.—

(1) PROHIBITION ON THE USE OF FUNDS.—No funds shall be made available under this Act to—

(A) a foreign country of concern; or

(B) any country, entity, or person—

(i) upon which sanctions are imposed by the United States Department of the Treasury; or

(ii) that is an entity or person on the Entity List maintained by the Bureau of Industry and Security of the Department of Commerce and set forth in Supplement No. 4 to part 744 of title 14, Code of Federal Regulations.

(2) VETTING.—The Secretary of State shall vet foreign government partners to determine whether there is credible information that such partner—

(A) has committed serious human rights abuses or engaged in corruption, as defined by section 1 of Executive Order 13818 (50 U.S.C. 1701 note; relating to blocking the property of persons involved in serious human rights abuse or corruption), or is determined to be ineligible for assistance pursuant to section 620M of the Foreign Assistance Act of 1961 (22 U.S.C. 2378d); and

(B) uses or is likely to use technologies outlined in subsection (c) and supported by this Act to engage in—

(i) violations of human rights;

(ii) targeted or bulk surveillance in violation of rule of law principles or fundamental freedoms;

(iii) the monitoring of journalists, activists, human rights defenders, opposition parties, or political dissidents;

(iv) internet shutdowns or to limit or control elections or protests;

(v) political censorship or the targeting and suppression of political speech or political opponents;

(vi) denial of access to technology or services based on race, ethnicity, gender, religion, or other discriminatory factors; and

(vii) acts of transnational repression.

(3) DISQUALIFICATION.—Any foreign government partner determined by the Secretary of State

to engage in the activities described in paragraph (2)(B) shall be ineligible for support or assistance under this Act.

(j) REGIONAL TECHNOLOGY OFFICERS.—The Secretary of State shall, to the maximum extent practicable, leverage the Department of State's Regional Technology Officer Program, pursuant to section 9508 of the Department of State Authorization Act of 2022 (22 U.S.C. 10305), to assist United States overseas missions in identifying foreign government partners to participate in the Program.

(k) FOREIGN COMMERCIAL OFFICERS.—As appropriate, the Secretary of State shall, in coordination with the Secretary of Commerce, seek to leverage the Foreign Commercial Officer Program to assist United States overseas missions in identifying foreign government partners to participate in the Program.

(l) CONGRESSIONAL NOTIFICATION REQUIREMENT.—Not later than 15 days before amounts from the Cyberspace, Digital Connectivity, and Related Technologies (CDT) Fund are obligated for purposes of carrying out this section, the Secretary of State shall submit notification of such obligation to—

(1) the Committee on Foreign Relations in the Senate;

(2) the Committee on Appropriations of the Senate;

(3) the Committee on Foreign Affairs in the House of Representatives; and

(4) the Committee on Appropriations of the House of Representatives.

(m) ANNUAL REPORT.—Not later than one year after the date of the enactment of this Act and annually thereafter, the Secretary of State, in coordination with the Secretary of Commerce, shall submit to the appropriate congressional committees a report that includes—

(1) a complete list of participating foreign government partners in the Program;

(2) progress and results achieved in the previous calendar year;

(3) the overall amount of purchases or investments each foreign government partner has made since initial participation in the Program;

(4) specific trusted cyber and digital technologies provided to participating foreign government partners, including—

(A) the name of the provider company or companies;

(B) the total value of the procurements;

(C) description of the capability; and

(D) how the procured capability addresses the original request submitted by the foreign government partner, if applicable;

(5) next steps for each participating foreign government partner in their respective Program pipeline;

(6) any challenges for a foreign government partner's participation in the Program, including how those challenges are being addressed; and

(7) how risks related to technology transfer, if applicable, are being mitigated.

(n) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $500,000,000 for fiscal year 2026 through fiscal year 2031 to the Cyberspace, Digital Connectivity, and Related Technologies (CDT) Fund under section 592 of the Foreign Assistance Act for Fiscal Year 1961 (22 U.S.C. 2349cc–1) for purposes of carrying out this section.

(o) SUNSET.—The Program and its associated authorities established under this section shall terminate on the date that is eight years after the date of the enactment of this Act.

SEC. 5. OFFICE OF UNITED STATES TECHNOLOGY PROCUREMENT.

(a) DESIGNATION OF RESPONSIBILITY.—The Secretary of State shall designate an existing office within the Bureau for Cyberspace and Digital Policy of the Department of State, or newly establish an Office of United States Technology Procurement (referred to in this Act as the ''Office''), which shall be responsible for administering the Program.

(b) PERSONNEL.—

(1) COMPOSITION.—The Office shall be comprised of a Director, a Deputy Director, and such other staff as the Secretary deems appropriate.

(2) STAFFING.—The Office shall include personnel with demonstrated expertise or experience in performing the following functions:

(A) Grant design and management.

(B) Program monitoring, evaluation, and learning.

(C) Cyber and digital technology commercialization, deployment, or procurement.

(3) DIRECTOR.—The Director of the Office shall fulfill the following responsibilities:

(A) Identify, on an annual basis, specific strategic priorities for the Program consistent with United States national security priorities and objectives.

(B) In coordination with the other relevant officials, select and approve all partnerships with foreign government partners under the Program.

(C) Conduct oversight, monitoring, and evaluation of the effectiveness of the Program, including long-term outcome assessments, to ensure the Program advances United States foreign policy and national security interests and to ensure monitoring, evaluation, and learning results directly inform future grant decisions.

(D) Ensure, to the maximum extent practicable, that all Program activities are carried out in coordination with other Federal efforts to promote the United States technology stack overseas.

(E) Compiling and submitting the list required by section 4(m).

(4) DEPUTY DIRECTOR.—The Deputy Director of the Office may have responsibility for policy and programming to assist the Director, particularly

with respect to coordination with other United States departments and agencies.

(c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $2,000,000 for fiscal years 2026 through 2028 for the purposes of implementing the Office.

SEC. 6. EXPANDING NECESSARY TECHNOLOGY AND RELATED EXPERTISE AT UNITED STATES OVERSEAS MISSIONS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that, for the United States Government to successfully implement the Program, it is vital that the United States recruit and retain the necessary talent to facilitate such partnerships.

(b) IN GENERAL.—The Secretary of State shall, to the maximum extent possible, take measures to ensure that United States overseas missions in countries that are participating in the Program host at least one full-time personnel with demonstrated proficiency in matters related to cybersecurity, technology, and other related expertise to sufficiently carry out the Program.

SEC. 7. EXTENDING AUTHORIZATION OF APPROPRIATIONS FOR THE REGIONAL TECHNOLOGY OFFICER PROGRAM.

Subsection (d) of section 9508 of the Department of State Authorization Act of 2022 (22 U.S.C. 10305) is amended by striking "2027" and inserting "2032".

SEC. 8. PRESERVING MARKET-BASED COMPETITION FOR CYBER AND DIGITAL TECHNOLOGIES.

(a) STATEMENT OF POLICY.—It is the policy of the United States to support market-based mechanisms for the export and adoption of United States cyber and digital technologies abroad, and to oppose state-directed or state-controlled economic models that risk to displace or crowd out private-sector competition in cyber and digital technology markets.

(b) IN GENERAL.—Nothing in this Act shall be construed to permit the Secretary of State, in coordination with other relevant Federal agencies, in carrying out the program outlined in section 4(a)—

(1) to unduly interfere with, or seek to substitute for, market-based competition among United States cyber and digital technology providers;

(2) to condition access to program support on the acceptance of commercial terms, partnerships, or business arrangements that United States cyber and

digital technology providers would not voluntarily accept in an arm's length commercial transaction; or

(3) to require foreign government partners to receive approval from the United States Government for procurements from United States cyber and digital technology providers pursued outside the Program, except as otherwise required by any other regulations or Federal law.

(c) CYBER AND DIGITAL TECHNOLOGY SMALL BUSINESS OWNERS.—Notwithstanding subsection (a), in carrying out the Program, the Secretary of State may provide targeted assistance, including capacity-building support and the facilitation of foreign government partner engagement, to United States small businesses and companies that lack the global reach, existing relationships, or resources to compete independently in foreign government partner procurement markets, provided that such assistance does not confer an unfair competitive advantage over other United States cyber and digital technology providers.

SEC. 9. GOVERNMENT ACCOUNTABILITY OFFICE REPORT.

Not later than one year after the date of the enactment of this Act, and not less frequently than every two years until the termination of the Program's authorities, the Comptroller General of the United States shall conduct and submit to the appropriate congressional committees a review of the Program. The review shall include an assessment of the Department of State's implementation of the Program, including—

(1) the Department of State's capacity to implement the Program, including personnel and budgetary resources;

(2) whether the Department of State has established the necessary processes and procedures to successfully achieve the Program objectives outlined in section 4;

(3) the Department of State's ability to conduct appropriate monitoring and evaluation of Program implementation;

(4) any technologies added or removed from the list under section 4(c) of covered cyber and digital technologies; and

(5) any other elements deemed necessary by the Comptroller General of the United States.

SEC. 10. FOREIGN SERVICE OFFICER TECHNOLOGY CAREER TRACK FEASIBILITY STUDY AND REPORT.

Not later than 1 year after the date of the enactment of this Act, the Secretary shall—

(1) conduct a study to determine the feasibility and advisability of establishing a dedicated technology policy career track or ''cone'' for Foreign Service officers; and

(2) submit a report containing a summary of the results of such study to the appropriate committees of Congress.

SEC. 11. DERIVATION OF FUNDS.

Amounts made available to carry out this Act shall be derived from amounts authorized to be appropriated or otherwise made available to the Department of State.