I

118TH CONGRESS
1ST SESSION

H. R. 6307

To prohibit certain actions and require reporting to defend against the economic and national security risks posed by foreign adversarial blockchain networks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 8, 2023

Mr. NUNN of Iowa (for himself and Ms. SPANBERGER) introduced the following bill; which was referred to the Committee on Foreign Affairs, and in addition to the Committees on Financial Services, Intelligence (Permanent Select), and Oversight and Accountability, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To prohibit certain actions and require reporting to defend against the economic and national security risks posed by foreign adversarial blockchain networks, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Creating Legal Accountability for Rogue Innovators and Technology Act of 2023'' or the ''CLARITY Act of 2023''.

SEC. 2. FINDINGS; SENSE OF CONGRESS.

(a) FINDINGS.—Congress finds the following:

(1) Blockchain service activities by governments and organizations that are adversaries of the United States can create risks to the economic, national security and foreign policy interests of the United States.

(2) The Blockchain-based Services Network of the People's Republic of China, and unregulated, self-proclaimed ''supra-national'' companies pose risks to the national security and foreign policy interests of the United States.

(b) SENSE OF CONGRESS.—It is the sense of Congress that the development of a Federal Government strategy to protect the United States from risks created from the Blockchain-based Services Network of the People's Republic of China and other foreign adversarial blockchain network infrastructure is essential to the national security and economic security of the United States.

SEC. 3. PROHIBITIONS RELATING TO COVERED DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAIN EQUIPMENT OR SERVICES.

(a) PROHIBITION ON ACQUISITION.—No head of an executive agency may acquire, or enter into, extend, or renew a contract or other agreement for, any equipment, system, or service that uses covered distributed ledger

technology and blockchain equipment or services as a substantial or essential component of, or critical technology as part of, such equipment, system, or service.

(b) PROHIBITION ON LOAN AND GRANT FUNDS.—

(1) PROHIBITION.—No head of an executive agency may obligate or expend loan or grant funds to acquire, or enter into, extend, or renew a contract or other agreement for, an equipment, system, or service described in subsection (a).

(2) PRIORITIZATION.—In implementing the prohibition under paragraph (1), the heads of executive agencies administering loan, grant, or subsidy programs, including the Secretary of Homeland Security and the Secretary of Commerce, shall prioritize available funding and technical support to assist affected businesses, institutions, and organizations as is reasonably necessary for those affected entities to transition from covered distributed ledger technology and blockchain equipment or services, to acquire replacement equipment and services, and to ensure that communications service to users and customers is sustained.

(c) RULE OF CONSTRUCTION.—Nothing in subsection (a) or (b) shall be construed to—

(1) prohibit the head of an executive agency from acquiring from an entity, or entering into, extending, or renewing a contract or other agreement with an entity for, a service that connects to the facilities of a third party, such as blockchain protocols, or interconnection arrangements; or

(2) cover wireless telecommunications equipment or third-party validators that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) EFFECTIVE DATE.—The prohibitions under subsections (a) and (b) shall take effect on the date that is 2 years after the date of the enactment of this Act.

(e) WAIVER AUTHORITY.—

(1) EXECUTIVE AGENCIES.—Except as provided in paragraph (2), beginning on the effective date under subsection (d), the head of an executive agency may, for a period of not more than 2 years per waiver, issue a waiver of the requirements under subsection (a) with respect to an entity that requests such a waiver. The waiver may be provided only if the entity seeking the waiver—

(A) provides a compelling justification for the additional time to implement the require-

ments under such subsection, as determined by the head of the executive agency; and

(B) submits to the head of the executive agency, who shall not later than 30 days thereafter submit to the appropriate congressional committees, a full and complete laydown of the presences of covered distributed ledger technology and blockchain equipment or services in the entity's supply chain and a phase-out plan to eliminate such covered distributed ledger technology and blockchain equipment or services.

(2) ELEMENTS OF THE INTELLIGENCE COMMUNITY.—Beginning on the effective date under subsection (d), each head of an element of the intelligence community may waive the requirements under subsection (a) if such head determines the waiver is in the national security interests of the United States.

SEC. 4. REPORTS TO DEFEND AGAINST RISKS POSED BY COVERED DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAIN EQUIPMENT OR SERVICES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter,

the Secretary of the Treasury, the Secretary of State, and the Director of National Intelligence shall jointly, and in consultation with the officials specified in subsection (b), submit to Congress a report that includes the following:

(1) A description of interagency policies and procedures to defend the United States financial markets, United States sanctions, United States business interests in the People's Republic of China, and global supply chains from the economic and national security risks posed by covered distributed ledger technology and blockchain equipment or services.

(2) A description of commercial and public administration activities used by the Government of the People's Republic of China and the Chinese Communist Party involving the entities listed under subparagraphs (A) through (E) of section 7(2), including militarization, industrialization, international trade, and other commercial activity.

(3) An assessment of the foreign policy and national security risks to the United States relating to transactions using covered distributed ledger technology and blockchain equipment or services, including circumvention of United States and international sanctions, including through the Society for World-

wide Interbank Financial Telecommunication (commonly known as ''SWIFT'') payments system.

(4) An assessment of data collection, cybersecurity risks, and the use of data that involves United States persons by the Government of the People's Republic of China and the Chinese Communist Party involving transactions relating to covered distributed ledger technology and blockchain equipment or services of the People's Republic of China.

(5) An assessment of the use of covered distributed ledger technology and blockchain equipment or services to collect data as part of the social credit system of the People's Republic of China.

(6) An assessment of the impact and national security risks of covered distributed ledger technology and blockchain equipment or services on data collection, cross-border payments, and economic integration, including with respect to countries participating in the Belt and Road Initiative of the People's Republic of China.

(7) An assessment of the impact of covered distributed ledger technology and blockchain equipment or services on the United States blockchain technology and distributed ledger technology industries, to include an assessment of its commercial adoption

globally and its integration with other smart city technologies in the United States and internationally.

(8) An assessment of the technologies, system architectures, and protocols underpinning covered distributed ledger technology and blockchain equipment or services, and recommendations with respect to strengthening export controls for United States technologies relating to the development and implementation of covered distributed ledger technology and blockchain equipment or services.

(9) An assessment of the impact of covered distributed ledger technology and blockchain equipment or services on international illicit finance.

(10) An assessment of the impact of covered distributed ledger technology and blockchain equipment or services on global trade, investment, and other activities and how increased use of covered distributed ledger technology and blockchain equipment or services may affect the status and future of the United States dollar as the world reserve currency.

(11) An assessment of how covered distributed ledger technology and blockchain equipment or services fit into the national security and economic objectives of the People's Republic of China and the

Chinese Communist Party, along with other foreign adversaries.

(12) An assessment of coordination between the United States and allies of the United States with respect to the national security risks and best practices relating to covered distributed ledger technology and blockchain equipment or services.

(13) Any other recommendations of the Secretary of Treasury, the Secretary of State, or the Director of National Intelligence regarding the foreign policy and national security implications of covered distributed ledger technology and blockchain equipment or services.

(b) OFFICIALS SPECIFIED.—The officials specified in this subsection include the following:

(1) The Secretary of Defense.

(2) The Secretary of Commerce.

(3) The United States Trade Representative.

(4) The Attorney General.

(5) The Chairman of the Board of Governors of the Federal Reserve System.

(6) The Director of the National Institute of Standards and Technology and the Under Secretary of Commerce for Standards and Technology.

(7) The Under Secretary of Commerce for Industry and Security of the United States.

(c) FORM.—Each report required by subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

SEC. 5. RECOMMENDATIONS FOR CONGRESS.

Not later than 90 days after each date on which a report is submitted under section 4, the Secretary of the Treasury, the Secretary of State, and the Director of National Intelligence shall jointly submit to Congress a set of recommendations that contain—

(1) a list of existing enforcement actions that may be used to defend the United States from risks identified in the report; and

(2) an action-item plan on steps Congress may take to address such risks.

SEC. 6. REPORT ON MALIGN ENTITIES IN BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY INDUSTRY.

(a) REPORT.—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Secretary of the Treasury, the Secretary of State, and the Director of National Intelligence shall jointly, and in consultation with the officials specified in section 5(b), submit to Congress a report that includes the following:

(1) A list of countries, proxies, firms, and technologies that are malign in the blockchain and distributed ledger technology industry.

(2) A description of what harms such countries, proxies, firms, and technologies cause to United States interests and sanctions enforcement, the use of the United States dollar, and international anti-money laundering and countering the financing of terrorism standards.

(3) A description of what mitigating strategies the United States may use to counter such harms.

(4) Recommendations on how to add to or modify the list of covered distributed ledger technology and blockchain equipment or services in order to capture new networks that emerge from foreign adversaries.

(b) FORM.—The report required by subsection (a) may be submitted in classified form, but if so submitted shall include an unclassified executive summary.

SEC. 7. DEFINITIONS.

In this Act:

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

(A) the Committee on Banking, Housing, and Urban Affairs, the Committee on Foreign Relations, and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Financial Services, the Committee on Foreign Affairs, the Committee on Intelligence, and the Committee on Oversight and Government Reform of the House of Representatives.

(2) COVERED DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAIN EQUIPMENT OR SERVICES.—The term ''covered distributed ledger technology and blockchain equipment or services'' means distributed ledger technology and blockchain equipment or services of or originating from a foreign adversary, including any of the following parent companies or subsidiaries thereof:

(A) The Blockchain-based Services Network.

(B) The Spartan Network.

(C) The Conflux Network.

(D) iFinex, Inc.

(E) Red Date Technology Co., Ltd.

(3) EXECUTIVE AGENCY.—The term ''executive agency'' has the meaning given the term in section 133 of title 41, United States Code.

(4) FOREIGN ADVERSARY.—The term ''foreign adversary'' has the meaning given such term in section 7.2 of title 15, Code of Federal Regulations.

(5) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

○