115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
115–984

FINANCIAL TECHNOLOGY PROTECTION ACT

SEPTEMBER 26, 2018.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. HENSARLING, from the Committee on Financial Services, submitted the following

R E P O R T

[To accompany H.R. 5036]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the bill (H.R. 5036) to establish an Independent Financial Technology Task Force, to provide rewards for information leading to convictions related to terrorist use of digital currencies, to establish a FinTech Leadership in Innovation Program to encourage the development of tools and programs to combat terrorist and illicit use of digital currencies, and for other purposes, having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

The amendments are as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Financial Technology Protection Act".

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that the Federal Government should prioritize the investigation of terrorist and illicit use of new financial technology, including digital currencies.

SEC. 3. INDEPENDENT FINANCIAL TECHNOLOGY TASK FORCE TO COMBAT TERRORISM AND ILLICIT FINANCING.

(a) ESTABLISHMENT.—There is established the Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing (the "Task Force"), which shall consist of—

(1) the Secretary of the Treasury, who shall serve as the head of the Task Force;
(2) the Attorney General;
(3) the Director of National Intelligence;
(4) the Director of the Financial Crimes Enforcement Network;
(5) the Director of the Secret Service;
(6) the Director of the Federal Bureau of Investigation; and

(7) 6 individuals appointed by the Secretary of the Treasury, in consultation with the members of the Task Force described under paragraphs (2) through (6), to represent the private sector (including the banking industry, nonprofit groups, and think tanks), with at least 2 of such individuals having experience in the Fintech industry.

(b) DUTIES.—The Task Force shall—

(1) conduct independent research on terrorist and illicit use of new financial technologies, including digital currencies; and

(2) develop legislative and regulatory proposals to improve counter-terrorist and counter-illicit financing efforts.

(c) ANNUAL CONGRESSIONAL REPORT.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the Task Force shall issue a report to the Congress containing the findings and determinations made by the Task Force in the previous year and any legislative and regulatory proposals developed by the Task Force.

SEC. 4. REWARDS FOR INFORMATION RELATED TO TERRORIST USE OF DIGITAL CURRENCIES.

(a) IN GENERAL.—The Secretary of the Treasury, in consultation with the Attorney General, shall establish a fund to pay a reward, not to exceed $450,000, to any person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies.

(b) USE OF FINES AND FORFEITURES.—With respect to fines and forfeitures related to the conviction of an individual involved with terrorist use of digital currencies, the Secretary of the Treasury shall, without further appropriation or fiscal year limitation—

(1) use such amounts to pay rewards under this section related to such conviction; and

(2) with respect to any such amounts remaining after payments are made under paragraphs (1) and (2), deposit such amounts in the FinTech Leadership in Innovation and Financial Intelligence Program.

SEC. 5. FINTECH LEADERSHIP IN INNOVATION AND FINANCIAL INTELLIGENCE PROGRAM.

(a) ESTABLISHMENT.—There is established a program to be known as the "Fintech Leadership in Innovation and Financial Intelligence Program", which shall be funded as provided under section 4(b)(2).

(b) INNOVATION GRANTS.—

(1) IN GENERAL.—The Secretary of the Treasury shall make grants for the development of tools and programs to detect terrorist and illicit use of digital currencies.

(2) ELIGIBLE RECIPIENTS.—The Secretary may make grants under this subsection to entities located in the United States, including academic institutions, companies, nonprofit institutions, individuals, and any other entities locating in the United States that the Secretary determines appropriate.

(3) ELIGIBLE PROJECTS.—With respect to tools and programs described under paragraph (1), in addition to grants for the development of such tools and programs, the Secretary may make grants under this subsection to carry out pilot programs using such tools, the development of test cases using such tools, and research related to such tools.

(4) PREFERENCES.—In making grants under this subsection, the Secretary shall give preference to—

(A) technology that is nonproprietary or that is community commons-based;

(B) computer code that is developed and released on an open source basis;

(C) tools that are proactive (such as meeting regulatory requirements under "know your customer" and anti-money laundering requirements for any entity that has to comply with U.S. Government regulations) vs. reactive (such as aiding law enforcement organizations in catching illegal activity after the fact); and

(D) tools and incentives that are on decentralized platforms.

(5) OTHER REQUIREMENTS.—

(A) USE OF EXISTING GLOBAL STANDARDS.—Any new technology developed with a grant made under this subsection shall be based on existing global standards, such as those developed by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C).

(B) SUPPORTING EXISTING LAWS OR REGULATIONS.—Tools and programs developed with a grant made under this subsection shall be in support of existing laws or regulations, including the Bank Secrecy Act, and make efforts to balance privacy and anti-money laundering concerns.

(C) OPEN ACCESS REQUIREMENT.—Tools and programs developed with a grant made under this subsection shall be freely accessible and usable by the public. This requirement may be fulfilled by publicly availing application programming interfaces or software development kits.

SEC. 6. PREVENTING ROGUE AND FOREIGN ACTORS FROM EVADING SANCTIONS.

(a) REPORT AND STRATEGY WITH RESPECT TO DIGITAL CURRENCIES AND OTHER RELATED EMERGING TECHNOLOGIES.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the President, acting through the Secretary of Treasury and in consultation with the Attorney General, the Secretary of State, the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Office of Management and Budget, and the appropriate Federal banking agencies and Federal functional regulators, shall—

(A) submit to the appropriate congressional committees a report that identifies and describes the potential uses of digital currencies and other related emerging technologies by states, non-state actors, and foreign terrorist organizations to evade sanctions, finance terrorism, or launder monetary instruments, and threaten United States national security; and

(B) develop and submit to the appropriate congressional committees a strategy to mitigate and prevent such illicit use of digital currencies and other related emerging technologies.

(2) FORM; PUBLIC AVAILABILITY.—

(A) FORM.—The report and strategy required under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

(B) PUBLIC AVAILABILITY.—The unclassified portion of such report and strategy shall be made available to the public and posted on the internet website of the Department of Treasury—

(i) in pre-compressed, easily downloadable versions that are made available in all appropriate formats; and

(ii) in machine-readable format, if applicable.

(3) SOURCES OF INFORMATION.—In preparing the report and strategy required under paragraph (1), the President may utilize any credible publication, database, web-based resource, and any credible information compiled by any government agency, nongovernmental organization, or other entity that is made available to the President.

(b) BRIEFING.—Not later than 2 years after the date of the enactment of this Act, the Secretary of the Treasury shall brief the appropriate congressional committees on the implementation of the strategy required under subsection (a).

SEC. 7. DEFINITIONS.

For purposes of this Act:

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

(A) the Committee on Financial Services, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, and the Committee on Foreign Affairs of the House of Representatives; and

(B) the Committee on Banking, Housing, and Urban Affairs, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, and the Committee on Foreign Relations of the Senate.

(2) APPROPRIATE FEDERAL BANKING AGENCIES.—The term "appropriate Federal banking agencies" has the meaning given the term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(3) BANK SECRECY ACT.—The term "Bank Secrecy Act" means—

(A) section 21 of the Federal Deposit Insurance Act;

(B) chapter 2 of title I of Public Law 91–508; and

(C) subchapter II of chapter 53 of title 31, United States Code.

(4) DIGITAL CURRENCY.—The term "digital currency"—

(A) means a digital representation of value that—

(i) is used as a medium of exchange, unit of account, or store of value; and

(ii) is not established legal tender, whether or not denominated in established legal tender; and

(B) does not include—

(i) a transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for legal tender, bank credit, or digital currency; or

(ii) a digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family

of games sold by the same publisher or offered on the same game platform.

(5) FEDERAL FUNCTIONAL REGULATOR.—The term "Federal functional regulator" has the meaning given that term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(6) FOREIGN TERRORIST ORGANIZATION.—The term "foreign terrorist organization" means an organization that is designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189).

(7) TERRORIST.—The term "terrorist" includes a person carrying out domestic terrorism or international terrorism (as such terms are defined, respectively, under section 2331 of title 18, United States Code).

Amend the title so as to read:

A bill to establish an Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing, to provide rewards for information leading to convictions related to terrorist use of digital currencies, to establish a Fintech Leadership in Innovation and Financial Intelligence Program to encourage the development of tools and programs to combat terrorist and illicit use of digital currencies, and for other purposes.

PURPOSE AND SUMMARY

On February 15, 2018 Representative Ted Budd introduced H.R. 5036, the "Financial Technology Protection Act". The legislation would establish an Independent Financial Technology Task Force to improve coordination between the private and public sectors to research and develop legislative and regulatory proposals to decrease terrorist and illicit use of new financial technologies, including digital currencies. This bill includes a Sense of Congress that, "the Federal Government should prioritize the investigation of terrorist and illicit use of new financial technology, including digital currencies." The bill would also require the Secretary of the Treasury, in consultation with the Attorney General, to establish a fund, not to exceed $450,000, to pay a reward to any person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies; and a "FinTech" Leadership in Innovation Program to provide grants for the development of the tools and programs to detect terrorist and illicit use of digital currencies.

BACKGROUND AND NEED FOR LEGISLATION

The goal of H.R. 5036 is to enable experts in the private sector and the government to research and report to Congress on how best to counter the illicit use of digital currencies.

Advances in technology and the widespread use of the Internet and mobile communication devices have helped fuel the growth in financial technology products and services. Digital currencies in particular can make for speedier, more secure, more cost-efficient, disintermediated, cross-border settlements of transactions. However, the national security implications of digital currency technology have increasingly been the subject of much debate. The rise of digital currency in the financial technology space has prompted expansive discussion about the nexus between the use of these systems and financial crime. The legislation is timely and as one witness noted in their June 7, 2017 testimony before the Subcommittee on Terrorism and Illicit Finance, "Unfortunately, this also means that, like the internet, it is open to bad actors who take

advantage of it. Criminals certainly use it today, and we have begun to see some nascent interest from terrorist groups." [1]

There have been a handful of instances in which terrorists have used digital currencies to raise funds, such as through solicited online donations using digital currencies. Criminal organizations are exploiting the pseudo-anonymity of some digital currencies through ransomware attacks and payment facilitation via online dark web forums like Alpha Bay and Silk Road. According to a report on the potential of terrorist use of digital currencies by the Center for a New American Security, however, "Currently there is no more than anecdotal evidence that terrorist groups have used virtual currencies to support themselves." [2]

The Royal United Services Institute (RUSI), the United Kingdom's leading defense and security think tank, released a paper in March 2017 about the nexus between digital currencies and financial crime following the European Union's 5th Anti-Money Laundering (AML) Directive. RUSI outlines that anonymity/pseudonymity; rapid international transaction settlement; and decentralization and contained environments are the main factors providing a number of financial crime risks from digital currencies. The Center for a New American Security (CNAS) also released a similar paper in May 2017 putting context around anecdotal evidence that terrorist groups have used digital currencies. The use of digital currencies by "lone wolf" terrorists is a "much bigger potential threat" according to CNAS because of the small scales of funding needed to execute attacks.

According to the RAND Corporation, "there is ample evidence that organized non-state actors—especially cybercriminals—use existing digital currencies." One of the most common criminal uses of digital currencies, particularly with Bitcoin, is in cases of ransomware, "where cybercriminals encrypt a victim's data and only release it upon payment in a VC [virtual currency]." The WannaCry ransomware attack on May 15, 2017, where over 200,000 computers across 150 countries were affected, reportedly only netted the hackers $50,000 in Bitcoin due to the rapid intervention of a security researcher in the United Kingdom. Had every victim met the hackers' initial demands, the losses could have exceeded $60,000,000. Another common criminal use of digital currencies is for the purchase of illicit goods and drugs via online services on so-called "dark net" forums including Silk Road and AlphaBay. Taken down in 2013, the Silk Road facilitated Bitcoin transactions, primarily for drugs, but also for stolen goods, forged documents, and hacking services. When a larger dark net marketplace, AlphaBay, was shut down in July 2017, the site had transactions exceeding $1 billion in Bitcoin and other virtual currencies.

As new financial products and technologies, including digital currency, continue to change, legislation is necessary so that those currencies are not used by illicit actors and terrorist organizations

[1] Testimony of Jerry Brito, Executive Director of Coin Center, before the Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance on "Financial Innovation and National Security Implications", June 8, 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-jbrito-20170608.pdf.

[2] Zachary K. Goldman et al., Terrorist Use of Virtual Currencies: Containing the Potential Threat, Center for a New American Security, May 2017, at page 2, available at https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies.

to escape a money trail. H.R. 5036 achieves this important objective.

HEARINGS

The Committee on Financial Services Subcommittee on Terrorism and Illicit Finance held a hearing examining matters relating to H.R. 5036 on June 8, 2017 and June 20, 2018.

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on July 24, 2018 and ordered H.R. 5036 to be reported favorably to the House as amended by a recorded vote of 57 yeas to 0 nays (recorded vote no. FC–197), a quorum being present. [Before the motion to report was offered, the Committee adopted an amendment in the nature of a substitute offered by Mr. Budd by voice vote.]

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The sole recorded vote was on a motion by Chairman Hensarling to report the bill favorably to the House as amended. The motion was agreed to by a recorded vote of 57 yeas to 0 nays (Record vote no. FC–197), a quorum being present.

Record vote no. FC-197

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Hensarling	X			Ms. Maxine Waters (CA)	X		
Mr. McHenry	X			Mrs. Carolyn B. Maloney (NY)	X		
Mr. King	X			Ms. Velázquez	X		
Mr. Royce (CA)	X			Mr. Sherman	X		
Mr. Lucas	X			Mr. Meeks	X		
Mr. Pearce	X			Mr. Capuano	X		
Mr. Posey	X			Mr. Clay	X		
Mr. Luetkemeyer	X			Mr. Lynch	X		
Mr. Huizenga	X			Mr. David Scott (GA)	X		
Mr. Duffy	X			Mr. Al Green (TX)	X		
Mr. Stivers	X			Mr. Cleaver	X		
Mr. Hultgren	X			Ms. Moore			
Mr. Ross	X			Mr. Ellison			
Mr. Pittenger	X			Mr. Perlmutter	X		
Mrs. Wagner	X			Mr. Himes	X		
Mr. Barr	X			Mr. Foster	X		
Mr. Rothfus	X			Mr. Kildee	X		
Mr. Messer	X			Mr. Delaney	X		
Mr. Tipton	X			Ms. Sinema	X		
Mr. Williams	X			Mrs. Beatty	X		
Mr. Poliquin	X			Mr. Heck	X		
Mrs. Love	X			Mr. Vargas	X		
Mr. Hill	X			Mr. Gottheimer	X		
Mr. Emmer	X			Mr. Gonzalez (TX)	X		
Mr. Zeldin	X			Mr. Crist	X		
Mr. Trott	X			Mr. Kihuen			
Mr. Loudermilk	X						
Mr. Mooney (WV)	X						
Mr. MacArthur	X						
Mr. Davidson	X						
Mr. Budd	X						
Mr. Kustoff (TN)	X						
Ms. Tenney	X						
Mr. Hollingsworth	X						

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the findings and recommendations of the Committee based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee states that H.R. 5036 will protect the use of digital currencies by providing for an Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing, Rewards for Innovation Related to Terrorist Use of Digital Currencies, a FinTech Leadership in Innovation and Financial Intelligence Program, and a Report and Strategy with Respect to Digital Currencies and Other Related Emerging Technologies.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATES

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 6, 2018.

Hon. JEB HENSARLING,
Chairman, Committee on Financial Services,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5036, the Financial Technology Protection Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

KEITH HALL,
Director.

Enclosure.

H.R. 5036—Financial Technology Protection Act

H.R. 5036 would establish within the Department of the Treasury an Independent Financial Technology Task Force. The task force members would include six representatives from federal agencies, and six from the private sector with experience in financial

technology. The task force would research and develop legislative and regulatory proposals to reduce the illicit use of financial technologies. The bill also would fund a whistle blower rewards program and a grant program aimed at curbing the use of digital currencies by terrorists.

Based on the cost of similar task forces, CBO estimates that implementing H.R. 5036 would require four employees annually at a total average annual cost of $300,000, plus additional expenses for overhead, supplies, and the expenses of nonfederal task force members. In total, CBO estimates that the task force would cost about $700,000 annually, or about $4 million over the 2018–2023 period.

Individuals using digital currencies for terrorist purposes are subject to fines and the forfeiture of property or assets. Those proceeds are recorded on the budget as revenues and can be spent without further appropriation. Under the bill, those revenues could be used by the task force to reward any person who provides information leading to the conviction of an individual involved with the terrorist use of digital currencies and to fund a grant program to develop tools and programs to detect the illicit use of digital currencies. Because those funds can already be spent under current law, CBO estimates that there would be no significant effect on direct spending.

Because enacting the bill would affect direct spending, pay-as-you-go procedures apply. Enacting the bill would not affect revenues.

CBO estimates that enacting H.R. 5036 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 5036 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

The CBO staff contact for this estimate is Matthew Pickford. The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

This information is provided in accordance with section 423 of the Unfunded Mandates Reform Act of 1995.

The Committee has determined that the bill does not contain Federal mandates on the private sector. The Committee has determined that the bill does not impose a Federal intergovernmental mandate on State, local, or tribal governments.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of the section 102(b)(3) of the Congressional Accountability Act.

EARMARK IDENTIFICATION

With respect to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee has carefully reviewed the provisions of the bill and states that the provisions of the bill do not contain any congressional earmarks, limited tax benefits, or limited tariff benefits within the meaning of the rule.

DUPLICATION OF FEDERAL PROGRAMS

In compliance with clause 3(c)(5) of rule XIII of the Rules of the House of Representatives, the Committee states that no provision of the bill establishes or reauthorizes: (1) a program of the Federal Government known to be duplicative of another Federal program; (2) a program included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139; or (3) a program related to a program identified in the most recent Catalog of Federal Domestic Assistance, published pursuant to the Federal Program Information Act (Pub. L. No. 95–220, as amended by Pub. L. No. 98–169).

DISCLOSURE OF DIRECTED RULEMAKING

Pursuant to section 3(i) of H. Res. 5, (115th Congress), the following statement is made concerning directed rule makings: The Committee estimates that the bill requires no directed rule makings within the meaning of such section.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This Section cites H.R. 5036 as the "Financial Technology Protection Act."

Section 2. Sense of Congress

It is the sense of Congress that the Federal Government should prioritize the investigation of terrorist and illicit use of new financial technology, including digital currencies.

Section 3. Independent financial technology task force to combat terrorism and illicit financing

The Task Force has the goal of improving coordination between the private and public sectors to research and develop legislative and regulatory proposals to decrease terrorist and illicit use of new financial technologies, including digital currencies. The Task Force is required to report to Congress its findings and determinations not later than one year after the enactment date of this Act.

The Task Force is comprised of the Secretary of the Treasury, the Attorney General, the Director of National Intelligence, the Director of the Financial Crimes Enforcement Network (FinCEN), the Director of the Secret Service, the Director of the Federal Bureau of Investigation (FBI), and six individuals from the private sector appointed by the Secretary of the Treasury, in consultation with members of the Task Force, at least two of which must have experience in the financial technology industry.

The Task Force shall conduct independent research on terrorist and illicit use of new financial technologies, including digital cur-

rencies, and develop legislative and regulatory proposals to improve counter-terrorist and counter-illicit financing efforts.

Section 4. Rewards for information related to terrorist use of digital currencies

The Secretary of the Treasury, in consultation with the Attorney General, to establish a fund, not to exceed $450,000, to pay a reward to any person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies. With respect to fines and forfeitures related to the conviction of an individual involved with terrorist use of digital currencies, the Secretary of the Treasury shall, without further appropriation or fiscal year limitation—use such amounts to pay rewards under this section related to such conviction; and with respect to any such amounts remaining after payments are made, deposit such amounts in the FinTech Leadership in Innovation and Financial Intelligence Program.

Section 5. FinTech leadership in innovation and financial intelligence program

The Secretary of the Treasury shall make grants for the development of tools and programs to detect terrorist and illicit use of digital currencies. The Secretary may make grants under this subsection to entities located in the United States, including academic institutions, companies, nonprofit institutions, individuals, and any other entities locating in the United States that the Secretary determines appropriate.

The Secretary may make grants to carry out pilot programs using such tools, the development of test cases using such tools, and research related to such tools. In making grants, the Secretary shall give preference to technology that is nonproprietary or that is community commons-based; computer code that is developed and released on an open source basis; tools that are proactive (such as meeting regulatory requirements under "know your customer" and anti-money laundering requirements for any entity that has to comply with U.S. Government regulations) vs. reactive (such as aiding law enforcement organizations in catching illegal activity after the fact); and tools and incentives that are on decentralized platforms.

Any new technology developed with a grant shall be based on existing global standards, such as those developed by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). Tools and programs developed with a grant shall be in support of existing laws or regulations, including the Bank Secrecy Act, and make efforts to balance privacy and anti-money laundering concerns. Tools and programs developed with a grant shall be freely accessible and usable by the public. This requirement may be fulfilled by publicly availing application programming interfaces or software development kits.

Section 6. Preventing rogue and foreign actors from evading sanctions

Not later than 180 days after the date of the enactment of this Act, the President, acting through the Secretary of Treasury and in consultation with the Attorney General, the Secretary of State,

the Secretary of Homeland Security, the Director of National Intelligence, the Director of the Office of Management and Budget, and the appropriate Federal banking agencies and Federal functional regulators, shall submit to the appropriate congressional committees a report that identifies and describes the potential uses of digital currencies and other related emerging technologies by states, non-state actors, and foreign terrorist organizations to evade sanctions, finance terrorism, or launder monetary instruments, and threaten United States national security; and develop and submit to the appropriate congressional committees a strategy to mitigate and prevent such illicit use of digital currencies and other related emerging technologies. The report and strategy shall be submitted in unclassified form, but may contain a classified annex. The unclassified portion of such report and strategy shall be made available to the public and posted on the internet website of the Department of Treasury.

Not later than two years after the date of the enactment of this Act, the Secretary of the Treasury shall brief the appropriate congressional committees on the implementation of the strategy.

Section 6. Definitions

The term "appropriate congressional committees" means the Committee on Financial Services, the Committee on the Judiciary, the Permanent Select Committee on Intelligence, and the Committee on Foreign Affairs of the House of Representatives; and the Committee on Banking, Housing, and Urban Affairs, the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Select Committee on Intelligence, and the Committee on Foreign Relations of the Senate.

The term "appropriate Federal banking agencies" has the meaning given the term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813). The term "Bank Secrecy Act" means section 21 of the Federal Deposit Insurance Act; chapter 2 of title I of Public Law 91–508; and subchapter II of chapter 53 of title 31, United States Code. The term "digital currency" means a digital representation of value that is used as a medium of exchange, unit of account, or store of value; and is not established legal tender, whether or not denominated in established legal tender; and does not include a transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for legal tender, bank credit, or digital currency; or a digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform.

The term "Federal functional regulator" has the meaning given that term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809). The term "foreign terrorist organization" means an organization that is designated as a foreign terrorist organization under section 219 of the Immigration and Nationality Act (8 U.S.C. 1189). The term "terrorist" includes a person carrying out domestic terrorism or international terrorism (as such terms are defined, respectively, under section 2331 of title 18, United States Code).

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

H.R. 5036 does not repeal or amend any section of a statute. Therefore, the Office of Legislative Counsel did not prepare the report contemplated by Clause 3(e)(1)(B) of rule XIII of the House of Representatives.

○