115TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
115–636

PROTECTING CHILDREN FROM IDENTITY THEFT ACT

APRIL 13, 2018.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BRADY of Texas, from the Committee on Ways and Means, submitted the following

R E P O R T

[To accompany H.R. 5192]

[Including cost estimate of the Congressional Budget Office]

The Committee on Ways and Means, to whom was referred the bill (H.R. 5192) to authorize the Commissioner of Social Security to provide confirmation of fraud protection data to certain permitted entities, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

79–006

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protecting Children from Identity Theft Act".

SEC. 2. REDUCING IDENTITY FRAUD.

(a) PURPOSE.—The purpose of this section is to reduce the prevalence of synthetic identity fraud, which disproportionally affects vulnerable populations, such as minors and recent immigrants, by facilitating the validation by permitted entities of fraud protection data, pursuant to electronically received consumer consent, through use of a database maintained by the Commissioner.

(b) DEFINITIONS.—In this section:

(1) COMMISSIONER.—The term "Commissioner" means the Commissioner of the Social Security Administration.

(2) FINANCIAL INSTITUTION.—The term "financial institution" has the meaning given the term in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

(3) FRAUD PROTECTION DATA.—The term "fraud protection data" means a combination of the following information with respect to an individual:

(A) The name of the individual (including the first name and any family forename or surname of the individual).

(B) The Social Security account number of the individual.

(C) The date of birth (including the month, day, and year) of the individual.

(4) PERMITTED ENTITY.—The term "permitted entity" means a financial institution or a service provider, subsidiary, affiliate, agent, contractor, or assignee of a financial institution.

(c) EFFICIENCY.—

(1) RELIANCE ON EXISTING METHODS.—The Commissioner shall evaluate the feasibility of making modifications to any database that is in existence as of the date of enactment of this Act or a similar resource such that the database or resource—

(A) is reasonably designed to effectuate the purpose of this section; and

(B) meets the requirements of subsection (d).

(2) EXECUTION.—The Commissioner shall establish a system to carry out subsection (a), in accordance with section 1106 of the Social Security Act. In doing so, the Commissioner shall make the modifications necessary to any database that is in existence as of the date of enactment of this Act or similar resource, or develop a database or similar resource.

(d) PROTECTION OF VULNERABLE CONSUMERS.—The database or similar resource described in subsection (c) shall—

(1) compare fraud protection data provided in an inquiry by a permitted entity against such information maintained by the Commissioner in order to confirm (or not confirm) the validity of the information provided, and in such a manner as to deter fraudulent use of the database or similar resource;

(2) be scalable and accommodate reasonably anticipated volumes of verification requests from permitted entities with commercially reasonable uptime and availability; and

(3) allow permitted entities to submit—

(A) one or more individual requests electronically for real-time machine-to-machine (or similar functionality) accurate responses; and

(B) multiple requests electronically, such as those provided in a batch format, for accurate electronic responses within a reasonable period of time from submission, not to exceed 24 hours.

(e) CERTIFICATION REQUIRED.—Before providing confirmation of fraud protection data to a permitted entity, the Commissioner shall ensure that the Commissioner has a certification from the permitted entity that is dated not more than 2 years before the date on which that confirmation is provided that includes the following declarations:

(1) The entity is a permitted entity.

(2) The entity is in compliance with this section.

(3) The entity is, and will remain, in compliance with its privacy and data security requirements, as described in title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) and as required by the Commissioner, with respect to information the entity receives from the Commissioner pursuant to this section.

(4) The entity will retain sufficient records to demonstrate its compliance with its certification and this section for a period of not less than 2 years.

(f) CONSUMER CONSENT.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, a permitted entity may submit a request to the database or similar resource described in subsection (c) only—

(A) pursuant to the written, including electronic, consent received by a permitted entity from the individual who is the subject of the request; and

(B) in connection with any circumstance described in section 604 of the Fair Credit Reporting Act (15 U.S.C. 1681b).

(2) ELECTRONIC CONSENT REQUIREMENTS.—For a permitted entity to use the consent of an individual received electronically pursuant to paragraph (1)(A), the permitted entity must obtain the individual's electronic signature, as defined in section 106 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7006). Permitted entities must develop and use an electronic signature process in accordance with all Federal laws and requirements as designated by the Commissioner.

(3) EFFECTUATING ELECTRONIC CONSENT.—No provision of law or requirement, including section 552a of title 5, United States Code, shall prevent the use of electronic consent for purposes of this subsection or for use in any other consent based verification under the discretion of the Commissioner.

(g) COMPLIANCE AND ENFORCEMENT.—

(1) AUDITS AND MONITORING.—

(A) IN GENERAL.—The Commissioner—

(i) shall conduct audits and monitoring to—

(I) ensure proper use by permitted entities of the database or similar resource described in subsection (c); and

(II) deter fraud and misuse by permitted entities with respect to the database or similar resource described in subsection (c); and

(ii) may terminate services for any permitted entity that prevents or refuses to allow the Commissioner to carry out the activities described in clause (i) and may terminate or suspend services for any permitted entity as necessary to enforce any violation of this section or of any certification made under this section.

(2) ENFORCEMENT.—

(A) IN GENERAL.—Notwithstanding any other provision of law, including the matter preceding paragraph (1) of section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)), any violation of this section and any certification made under this section shall be enforced in accordance with paragraphs (1) through (7) of such section 505(a) by the agencies described in those paragraphs.

(B) RELEVANT INFORMATION.—Upon discovery by the Commissioner of any violation of this section or any certification made under this section, the Commissioner shall forward any relevant information pertaining to that violation to the appropriate agency described in subparagraph (A) for evaluation by the agency for purposes of enforcing this section.

(h) RECOVERY OF COSTS.—

(1) IN GENERAL.—

(A) IN GENERAL.—Amounts obligated to carry out this section shall be fully recovered from the users of the database or verification system by way of advances, reimbursements, user fees, or other recoveries as determined by the Commissioner. The funds recovered under this paragraph shall be deposited as an offsetting collection to the account providing appropriations for the Social Security Administration, to be used for the administration of this section without fiscal year limitation.

(B) PRICES FIXED BY COMMISSIONER.—The Commissioner shall establish the amount to be paid by the users under this paragraph, including the costs of any services or work performed, such as any appropriate upgrades, maintenance, and associated direct and indirect administrative costs, in support of carrying out the purposes described in this section, by reimbursement or in advance as determined by the Commissioner. The amount of such prices shall be periodically adjusted by the Commissioner to ensure that amounts collected are sufficient to fully offset the cost of the administration of this section.

(2) INITIAL DEVELOPMENT.—The Commissioner shall not begin development of a verification system to carry out this section until the Commissioner determines that amounts equal to at least 50 percent of program start-up costs have been collected under paragraph (1).

(3) EXISTING RESOURCES.—The Commissioner of Social Security may use funds designated for information technology modernization to carry out this section, but in all cases shall be fully reimbursed under paragraph (1)(A).

(4) ANNUAL REPORT.—The Commissioner of Social Security shall annually submit to the Committee on Ways and Means of the House of Representatives and the Committee on Finance of the Senate a report on the amount of indirect costs to the Social Security Administration arising as a result of the implementation of this section.

I. SUMMARY AND BACKGROUND

A. PURPOSE AND SUMMARY

The Protecting Children from Identity Theft Act (H.R. 5192), as reported by the Committee on Ways and Means, requires the Social Security Administration (SSA) to match the name, Social Security number (SSN), and date of birth submitted by permitted entities against the SSA's records. The bill seeks to protect individuals, firms and the economy by allowing financial institutions to verify the accuracy of their customers' personal identity information, in order to guard against the establishment of synthetic identities based on a valid SSN and a false name.

The bill would require the SSA to develop or improve an existing system which verifies name-SSN matches and require SSA to accept an electronic signature as authorization of the consent required to conduct this verification. Currently, the SSA requires a wet signature on a paper form as proof of consent. However, many credit applications occur online where a wet signature cannot be obtained.

The bill protects the confidentiality of consumers' information and guards against fraudulent misuse of the system by requiring valid consent; limiting the system to certified users; requiring users to comply with requirements for data security and privacy in federal law and as required by the Commissioner; requiring compliance audits of users; and authorizing the Commissioner to terminate or suspend verification services for users that do not comply with these requirements.

The bill also ensures the verification system does not detract from the SSA's ability to conduct its mission-critical work, by requiring users of the system to pay for all start-up and ongoing costs, both direct and indirect, of the verification system.

B. BACKGROUND AND NEED FOR LEGISLATION

Synthetic identity fraud is a form of identity theft that begins when fraudsters combine a real SSN and fictitious information, such as a name and date of birth, to apply for credit. Even though the financial institution may reject this initial application, credit bureaus create a record from this transaction based on the fraudulent credentials. This record can then be nurtured by the fraudster over time to establish a synthetic identity based on the valid SSN but false name, which eventually is used to commit financial or other fraud.

Synthetic identity fraud is a growing form of identity theft. According to TransUnion, a record $355 million in outstanding credit card balances was owed by "people" whom it suspects did not exist in 2017, up more than eightfold from 2012.[1] Synthetic identity fraud accounted for 85 percent of all identity fraud, 80 percent of

[1] *The New ID Theft: Millions of Credit Applicants Who Don't Exist*, The Wall Street Journal, (March 2018).

all credit card fraud losses, and 74 percent of the total dollars lost by U.S. business in 2014.[2] In 2016, credit card companies had approximately $1 billion in losses due to synthetic identity fraud.[3]

Children and other individuals with limited or non-existent credit histories are especially vulnerable to having their SSNs misused for a synthetic identity. Since children do not work, drive, or establish credit, an identity thief can misuse a child's SSN for a longer period of time before being noticed. According to the Detroit Free Press, over one million children have their identity stolen annually.[4] Children are 50 times more likely than adults to be identity theft victims, according to a study by Carnegie Mellon's CyLab.[5]

The Privacy Act and Social Security law set forth circumstances under which consumers can give consent for information about them held in government records to be shared. SSA has verified for private companies whether an individual's name, SSN and date of birth matches agency records since 2002. From 2002 to 2005, the SSA conducted a pilot program, the Social Security Number Verification Pilot for Private Business, to verify names and SSNs against the SSA's records for companies. The SSA launched the Consent Based Social Security Number Verification system (CBSV) in fiscal year (FY) 2009. Using CBSV, authorized users can verify the name, SSN, and date of birth of consenting individuals. CBSV responds with a match verification of "yes" or "no," and if records show that the SSN holder is deceased, CBSV returns a death indicator. The SSA does not respond with the reason for the mismatch, nor does it provide corrected information. Users enroll and agree to the terms and conditions in the SSA's CBSV User Agreement. Users must pay an enrollment fee of $5,000 plus an additional fee of $1.00 for each verification request. Since 2008, the SSA has processed about 16 million verification requests for 78 enrolled users. In FY 2017, the SSA completed 2,875,770 verification requests through CBSV. The SSA determined that 147,100 of those requests, or 5.1 percent, did not match the SSA's records. In addition to those mismatches, there were 100 instances where the SSA's records indicated the individual was deceased.

The user is required to obtain consent from the individual for SSA to provide the verification. However, the SSA requires the user to obtain the individual's wet signature, on the SSA's paper form SSA–89, to demonstrate consent. Since the SSA does not accept electronic consent, the CBSV is only useful in situations where the user can obtain and retain a signature on a paper form. (The user does not submit the signed form to SSA, but is required to retain it in its own records.) As a result, CBSV is of limited use for transactions that are done in real time without paper documentation, as is the case with most modern financial transactions.

Under a previous version of the user agreement, users were required to hire an independent Certified Public Accountant (CPA) to conduct compliance reviews to ensure they were following the re-

---

[2] *Synthetic Identity Fraud A Fast Growing Category*, Information Week, (October 2014).

[3] *Highlights of a Forum—Combating Synthetic Identity Fraud*, Government Accountability Office, (July 2017).

[4] *1.3 million kids have identity stolen annually*, 50% under 6-years-old, Detroit Free Press, (August 2016).

[5] *New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers*, Carnegie Mellon CyLab, (2011).

quirements of the agreement, including the consent requirement.[6] However, an October 2012 audit by the SSA's Office of the Inspector General determined that the "SSA did not always require that participating companies conduct an annual compliance review to ensure companies were complying with the terms and conditions of the User Agreement, especially the consent requirement."[7] The SSA has since strengthened its compliance procedures, and the SSA now contracts with a CPA firm to conduct annual onsite compliance reviews of every CBSV user. According to the SSA, during the most recent audit in FY 2016, 14 out of 72 audited users (19 percent) had instances of missing consent forms. In addition, 6 users (8 percent) had instances of consent forms that were unsigned, and 9 users (13 percent) had instances of accepting an electronically-signed consent form, without a wet signature.

C. Legislative History

BACKGROUND

H.R. 5192 was introduced on March 7, 2018, and was referred to the Committee on Ways and Means. The bill was introduced as a companion bill to section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (S. 2155).

COMMITTEE HEARINGS

None.

COMMITTEE ACTION

The Committee on Ways and Means marked up H.R. 5192, the Protecting Children from Identity Theft Act, on April 11, 2018, and ordered the bill, as amended, favorably reported (with a quorum being present).

II. EXPLANATION OF THE BILL

A. Short Title (Section 1 of Bill)

PRESENT LAW

No provision.

REASON FOR CHANGE

The Committee believes that the short title reflects the policy and intent included in the legislation.

EXPLANATION OF PROVISIONS

This section contains the short title of the bill, the "Protecting Children from Identity Theft Act."

EFFECTIVE DATE

The provision is effective upon the date of enactment.

---

[6] *User Agreement Between the Social Security Administration (SSA) And (Requesting Party) for Consent Based Social Security Number Verification (CBSV)*, Social Security Administration, (October 2016).

[7] *Monitoring Controls for the Consent Based Social Security Number Verification Program*, Office of the Inspector General, Social Security Administration, (October 2012). A–03–12–11201.

B. Reducing Identity Fraud (Section 2 of Bill)

PRESENT LAW

The Privacy Act, the Social Security Act, and other laws guard the confidentiality of information about individuals maintained by the government. They also set forth circumstances under which consumers can give consent for this information to be shared. Using this authority, the SSA established the CBSV to permit authorized users to verify whether an individual's name, SSN and date of birth match SSA's records, if the individual has given consent.

REASON FOR CHANGE

The Committee believes that Americans must be protected from all forms of identity theft. Because SSA is the agency which issues SSNs to individuals and maintains these records, it is in a unique position to help guard against the growing problem of synthetic identity fraud. The Protecting Children from Identity Theft Act will facilitate the verification of name-SSN matches against this authoritative source, with the individual's consent, and thus will help to combat synthetic identity fraud. The SSA's current CBSV is not useful for many types of financial transactions because it requires consent in the form of a wet signature. By requiring SSA to accept electronic consent, with appropriate safeguards, the legislation allows access for entities that conduct business online and electronically, thus protecting SSNs more widely.

EXPLANATION OF PROVISIONS

The SSA must establish a system to validate the name, SSN, and date of birth of an individual, if submitted by an authorized, permitted entity who has the consent of the individual, for purposes related to circumstances under which consumer reports may be provided under the Fair Credit Reporting Act. In establishing the verification system, the Commissioner may update a current SSA system, such as CBSV, or develop a new one. Permitted entities include financial institutions and their service providers, subsidiaries, affiliates, agents, contractors or assignees. The individual's consent may be obtained electronically, in accordance with federal e-signature laws, other relevant laws such as the Privacy Act, and in compliance with requirements specified by the Commissioner so as to ensure that the consent is valid and the individual providing it is authenticated by the entity.

The SSA's existing verification system, CBSV, was established under existing SSA authority, which was not changed by the legislation. It has a variety of users, including those who qualify as permitted entities under this legislation. The Committee recognizes the importance of CBSV to users and notes the legislation does not prohibit access to the improved verification system by other users, provided that those users also meet all SSA and Privacy Act requirements.

The system must be scalable and be able to accommodate reasonably anticipated volumes of verification requests, with commercially reasonable uptime and availability. Users are permitted to send individual or multiple requests to the SSA, via electronic

means. The Commissioner must provide the match/no-match response in real time, or within 24 hours in the case of batch-format requests.

While the Committee recognizes the importance of timely responses to verification requests, the SSA must design the system in such a way as to deter fraudulent use of the system. One potential for misuse is a user who tries to guess an individual's identifying information by submitting multiple, iterative verification requests in an attempt to eventually discover a valid name-number match. The Committee expects the SSA to monitor verification requests from users, and to take action against users who appear to be using the system in this or other fraudulent ways.

The ability of financial institutions to receive real-time responses is critical to combatting synthetic identity fraud. The Committee's intent is to provide a workable and efficient mechanism that protects children and other vulnerable populations from synthetic identity fraud, and that reflects the operational environment of the modern financial services industry, while protecting the SSA's ability to ensure the confidentiality and security of Americans' personal identity information.

The SSA requires users of CBSV to sign and comply with a user agreement that details the terms and conditions for use of the system. In order to ensure that only authorized entities have access to the verification system established by the legislation, that they are obtaining valid consent from individuals, and that they are adhering to privacy and data security standards, the Committee expects the SSA to establish a user agreement for the new system, using similar requirements and protections to those already in place for CBSV. The language provides that permitted entities must adhere to privacy and data security standards, as well as authentication and electronic signature standards, required by the Commissioner of Social Security. The Committee expects that these standards would be based on Federal laws, such as the Privacy Act, and related guidance, under which the Commissioner is required to protect the security and integrity of personal information in Social Security records and prevent against its unauthorized disclosure.

Users must have a valid certification with the SSA in order to receive verifications. The certification must be dated not more than two years prior to the date of the verification provided to the user. The certification must state that the user is a permitted entity; that it is in compliance with the provisions of the legislation; that it is in and will maintain compliance with privacy and data security requirements in banking law, and as required by the Commissioner; and that it will retain sufficient records to demonstrate compliance for at least two years. The Committee expects the SSA to effectively manage and track user certifications to ensure it only provides verifications to users with a valid certification. The SSA's authority regarding privacy and data security requirements for users is limited to their use of the verification system, including their use of data received from the new system, and does not extend to other activities of the users.

The Commissioner is required to audit and monitor users to ensure they are complying with the requirements of the law and the user agreement. The Commissioner has the authority to terminate or suspend verification services for users who do not cooperate with

such audits or monitoring, or to enforce any violation of the law, user agreement, or certification. It is the Committee's expectation that SSA will exercise its monitoring and enforcement authority promptly to protect consumers' information.

In addition to the Commissioner's authority to terminate or suspend a user's access, bank regulatory agencies also have enforcement authority regarding violations of the legislation. The Commissioner is required to report any violation to the appropriate regulatory agency.

The Committee does not intend for the implementation of the verification system to interfere with the SSA's ability to conduct its primary mission, which is to serve the American public by administering Social Security, Supplemental Security Income, and parts of Medicare. Thus, users of the verification system are required under the legislation to pay for all start-up and ongoing costs, including all direct and indirect costs, through fees as determined by the Commissioner. Development of the system may not begin until at least fifty percent of all projected start-up costs has been collected via fees; however, the Committee expects that the SSA will establish and implement the new system as quickly as possible thereafter. If additional funds are necessary to develop the system, the Commissioner may temporarily draw on funds from SSA's Limitation on Administrative Expenses account designated for information technology modernization; however, these expenditures shall be fully reimbursed via fees, so that all funds appropriated for information technology modernization are ultimately used for that purpose. The SSA will also provide an annual report to the Committee on Ways and Means and the Senate Finance Committee on the indirect costs associated with this new workload.

EFFECTIVE DATE

The provision is effective upon the date of enactment.

III. VOTES OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the following statement is made concerning the vote of the Committee on Ways and Means in its consideration of H.R. 5192, the Protecting Children from Identity Theft Act, on April 11, 2018.

The Chairman's amendment in the nature of a substitute was adopted by a voice vote (with a quorum being present).

The bill, H.R. 5192, was ordered favorably reported as amended by a roll call vote of 38 yeas to 0 nays (with a quorum being present). The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Brady	X			Mr. Neal	X		
Mr. Johnson	X			Mr. Levin	X		
Mr. Nunes	X			Mr. Lewis	X		
Mr. Reichert	X			Mr. Doggett	X		
Mr. Roskam	X			Mr. Thompson	X		
Mr. Buchanan	X			Mr. Larson	X		
Mr. Smith (NE)	X			Mr. Blumenauer	X		
Ms. Jenkins	X			Mr. Kind	X		
Mr. Paulsen	X			Mr. Pascrell	X		
Mr. Marchant	X			Mr. Crowley	X		
Ms. Black	X			Mr. Davis	X		

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Mr. Reed				Ms. Sanchez	X		
Mr. Kelly	X			Mr. Higgins	X		
Mr. Renacci	X			Ms. Sewell	X		
Mr. Meehan	X			Ms. DelBene	X		
Ms. Noem				Ms. Chu	X		
Mr. Holding	X						
Mr. Smith (MO)	X						
Mr. Rice	X						
Mr. Schweikert	X						
Ms. Walorski	X						
Mr. Curbelo	X						
Mr. Bishop	X						
Mr. LaHood	X						

IV. BUDGET EFFECTS OF THE BILL

A. Committee Estimate of Budgetary Effects

In compliance with clause 3(d) of rule XIII of the Rules of the House of Representatives, the following statement is made concerning the effects on the budget of the bill, H.R. 5192, as reported. The Committee agrees with the estimate prepared by the Congressional Budget Office (CBO), which is included below.

B. Statement Regarding New Budget Authority and Tax Expenditures Budget Authority

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee states that the bill involves no new or increased budget authority. The Committee states further that the bill involves no new or increased tax expenditures.

C. Cost Estimate Prepared by the Congressional Budget Office

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, requiring a cost estimate prepared by the CBO, the following statement by CBO is provided.

U.S. Congress,
Congressional Budget Office,
Washington, DC, April 12, 2018.

Hon. Kevin Brady,
Chairman, Committee on Ways and Means,
House of Representatives, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5192, the Protecting Children from Identity Theft Act.

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

Sincerely,

Keith Hall, *Director.*

Enclosure.

H.R. 5192—Protecting Children from Identity Theft Act

The Social Security Administration (SSA) operates the Consent Based Social Security Number Verification (CBSV) service, a fee-based program that allows financial institutions to verify that their

records of a person's name, date of birth, and Social Security Number match SSA's data. SSA tells institutions only whether the data does or does not match; no other detail is provided. The fees are classified as offsetting collections that are credited against SSA's discretionary appropriations.

H.R. 5192 would change the CBSV program by allowing people to electronically verify their consent to allow SSA to provide this information, rather than with a physical signature. CBO expects that change would expand the number of verification requests submitted to SSA.

Under H.R. 5192, SSA would set fees to equal the total administrative costs of the program. SSA would incur the direct costs of administering the service and the indirect costs in some cases of resolving errors that are discovered. CBO projects that fees would, on average, fully offset SSA's administrative costs. However, in any given fiscal year, the total amount of fees collected probably would differ slightly from actual costs.

CBO estimates that implementing the bill would result in net costs or savings of less than $500,000 in each year; the total effect would be negligible over the 2019–2028 period.

Enacting H.R. 5192 would not affect direct spending; therefore, pay-as-you-go procedures do not apply.

CBO estimates that enacting H.R. 5192 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2029.

H.R. 5192 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act.

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

V. OTHER MATTERS TO BE DISCUSSED UNDER THE RULES OF THE HOUSE

A. Committee Oversight Findings and Recommendations

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee made findings and recommendations that are reflected in this report.

B. Statement of General Performance Goals and Objectives

With respect to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee advises that the bill does not authorize funding, so no statement of general performance goals and objectives is required.

C. Information Relating to Unfunded Mandates

This information is provided in accordance with section 423 of the Unfunded Mandates Reform Act of 1995 (Pub. L. No. 104–4).

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.

D. Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits

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.

E. 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).

F. Disclosure of Directed Rule Makings

In compliance with Sec. 3(i) of H. Res. 5 (115th Congress), the following statement is made concerning directed rule makings: The Committee advises that the bill requires no directed rulemakings within the meaning of such section.

○