Calendar No. 491

118TH CONGRESS
2D SESSION

S. 3594

[Report No. 118–213]

To require governmentwide source code sharing, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 16, 2024

Mr. CRUZ (for himself, Mr. PETERS, and Mr. WYDEN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

SEPTEMBER 9, 2024

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To require governmentwide source code sharing, 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 "Source code Harmonization And Reuse in Information Technology Act" or the "SHARE IT Act".~~

~~SEC. 2. FINDINGS; PURPOSE.~~

~~(a) FINDINGS.—~~

~~(1) IN GENERAL.—Congress finds the following:~~

~~(A) DUPLICATION OF EFFORTS.—Federal agencies often engage in the development or procurement of similar software solutions for comparable problems, leading to a duplicative allocation of resources that could otherwise be avoided.~~

~~(B) COST INEFFICIENCY.—The absence of a mechanism for inter-agency source code sharing results in the Federal Government incurring unnecessary costs for software development, licensing, and maintenance, an inefficiency highlighted by the Government Accountability Office in numerous reports, including—~~

~~(i) Government Accountability Office Report "Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide" (GAO–14–413), published on May 22, 2014;~~

~~(ii) Government Accountability Office Report "2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve~~

~~Other Financial Benefits" (GAO–16–375SP), published on April 13, 2016;~~

~~(iii) Government Accountability Office Report "Information Technology: DoD Needs to Fully Implement Program for Piloting Open Source Software" (GAO–19–457), published on September 10, 2019;~~

~~(iv) Government Accountability Office Report "Information Technology: Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity" (GAO–20–691T), published on August 3, 2020; and~~

~~(v) Government Accountability Office Report "DoD Software Licenses: Better Guidance and Plans Needed to Ensure Restrictive Practices are Mitigated" (GAO–23–106290), published on September 12, 2023.~~

~~(C) TECHNOLOGICAL FRAGMENTATION.—The isolated development efforts of each agency contribute to a landscape of fragmented technologies that impede interoperability and data exchange between Federal systems.~~

~~(D) SLOW ADOPTION OF BEST PRACTICES.—The lack of software sharing hinders the diffusion of engineering best practices and innovations across agencies, whereas learning from the successes and failures of other agencies would accelerate the modernization of government systems.~~

~~(E) SECURITY VULNERABILITIES.—Redundant development efforts mean that security weaknesses inadvertently introduced in the software of an agency could go unnoticed by other agencies, whereas a shared codebase would benefit from collective security auditing and updates.~~

~~(F) PUBLIC ACCOUNTABILITY.—Software funded by taxpayers should be available for scrutiny by the public to the greatest extent possible, to ensure transparency and accountability.~~

~~(G) PILOT SUCCESS.—Preliminary initiatives aimed at making federally funded custom-developed code freely available to the public have demonstrated the viability and benefits of such sharing schemes, including—~~

~~(i) Memorandum M–16–21 issued by the Office of Management and Budget on August 8, 2016, entitled "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software"; and~~

~~(ii) "Code.gov", which documents how agencies already extensively use public repositories, demonstrating the ability of agencies to share code using existing infrastructure.~~

~~(2) CONCLUSION.—Based on the findings in paragraph (1), it is imperative for Congress to enact legislation that mandates the sharing of custom-developed code across agencies to promote efficiency, reduce waste, enhance security, and foster innovation in the Federal information technology ecosystem.~~

~~(b) PURPOSE.—The overarching aim of this Act is to maximize efficiency, minimize duplication, and enhance security and innovation across Federal agencies by requiring the sharing of custom-developed code between agencies by—~~

~~(1) enabling agencies to benefit mutually from the investments of other agencies in custom-developed code;~~

~~(2) promoting technological consistency and interoperability among agencies, thereby facilitating seamless data exchange and system integration;~~

~~(3) fostering a culture of sharing engineering best practices and successful technological innovations among agencies;~~

~~(4) enhancing transparency by making federally funded custom-developed code available for public scrutiny, subject to necessary security considerations; and~~

~~(5) leveraging inter-agency collaboration for better security auditing of the shared codebase, aiming for a more unified and secure technological infrastructure across agencies.~~

~~SEC. 3. DEFINITIONS.~~

~~In this Act:~~

~~(1) AGENCY.—The term "agency" has the meaning given that term in section 3502 of title 44, United States Code.~~

~~(2) CUSTOM-DEVELOPED CODE.—The term "custom-developed code"—~~

~~(A) means source code that is—~~

~~(i) produced in the performance of a Federal contract or is otherwise fully funded by the Federal Government; or~~

~~(ii) developed by a Federal employee as part of the official duties of the employee;~~

~~(B) includes—~~

~~(i) source code, or segregable portions of source code, for which the Federal Government could obtain unlimited rights under part 27 of the Federal Acquisition Regulation or any relevant supplemental acquisition regulations of an agency; and~~

~~(ii) source code written for a software project, module, plugin, script, middleware, or application programming interface; and~~

~~(C) does not include—~~

~~(i) source code that is solely exploratory or disposable in nature, including source code written by a developer experimenting with a new language or library; or~~

~~(ii) commercial off-the-shelf software or configuration scripts for such software.~~

~~(3) FEDERAL CHIEF INFORMATION OFFICER.—The term "Federal Chief Information Officer"~~

~~means the Administrator of the Office of Electronic Government.~~

~~(4) FEDERAL EMPLOYEE.—The term "Federal employee" has the meaning given the term "employee" in section 2105(a) of title 5, United States Code.~~

~~(5) METADATA.—The term "metadata", with respect to custom-developed code—~~

~~(A) has the meaning given that term in section 3502 of title 44, United States Code; and~~

~~(B) includes information on whether the custom-developed code—~~

~~(i) was produced pursuant to a contract, and the contract number, if any; and~~

~~(ii) is shared in a public or private repository, and includes a hyperlink to the repository, as applicable.~~

~~(6) PRIVATE REPOSITORY.—The term "private repository" means a software storage location—~~

~~(A) that contains source code, documentation, and other files; and~~

~~(B) access to which is restricted to authorized users.~~

~~(7) PUBLIC REPOSITORY.—The term "public repository" means a software storage location—~~

~~(A) that contains source code, documentation, and other files; and~~

~~(B) access to which is open to the public.~~

~~(8) SOFTWARE.—The term "software" has the meaning given the term "computer software" in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.~~

~~(9) SOURCE CODE.—The term "source code" means a collection of computer commands written in a computer programming language that a computer can execute as a piece of software.~~

~~SEC. 4. SOFTWARE REUSE.~~

~~(a) SHARING.—Not later than 210 days after the date of enactment of this Act, the head of each agency shall ensure that—~~

~~(1) the custom-developed code of the agency is contained at not less than 1 public or private repository and is accessible to Federal employees via procedures developed under subsection (d)(1)(A)(ii)(III); and~~

~~(2) all software and other key technical components, including documentation, data models,~~

~~schemas, metadata, and architecture designs, are owned by the agency.~~

~~(b) SOFTWARE REUSE RIGHTS IN PROCUREMENT CONTRACTS.—~~

~~(1) IN GENERAL.—The head of an agency that enters into a contract for the custom development of software shall acquire and enforce rights sufficient to enable the governmentwide access, execution, and modification of the custom-developed code relating to the software.~~

~~(2) BEST PRACTICES.—~~

~~(A) CONTRACT ADMINISTRATION.—With respect to a contract described in paragraph (1), the head of an agency shall ensure appropriate contract administration and use of best practices to secure the full scope of licenses and rights for the Federal Government of the custom-developed code developed under the contract, to allow for access, execution, and modification by other agencies.~~

~~(B) DEVELOPMENT PROCESS.—With respect to a contract described in paragraph (1), the head of an agency shall ensure the use of best practices to require and obtain the delivery of the custom-developed code, documentation of~~

~~the custom-developed code, configuration and artifacts required to develop, build, test, and deploy the custom-developed code, and other associated materials from the developer throughout the development process.~~

~~(c) DISCOVERY.—Not later than 210 days after the date of enactment of this Act, the head of each agency shall make metadata for the custom-developed code of the agency publicly accessible.~~

~~(d) ACCOUNTABILITY MECHANISMS.—~~

~~(1) AGENCY CIOS.—Not later than 180 days after the date of enactment of this Act, the Chief Information Officer of each agency, in consultation with the Chief Acquisition Officer, or similar official, of the agency and the Federal Chief Information Officer, shall develop an agency-wide policy that—~~

~~(A) addresses the requirements of this Act, including—~~

~~(i) ensuring that agency custom-developed code follows best practices for operating repositories and version control systems to keep track of changes and to facilitate collaboration among multiple developers;~~

~~(ii) managing the sharing and discovery of source code, including developing—~~

~~(I) procedures to determine whether any custom-developed code meets the conditions for an exemption under this Act;~~

~~(II) procedures for making metadata for custom-developed code discoverable, pursuant to section 4(c);~~

~~(III) procedures for Federal employees to discover and gain access to private repositories;~~

~~(IV) standardized reporting practices across the agency to capture key information relating to a contract for reporting statistics about the contract; and~~

~~(V) procedures for updating metadata, private repositories, and public repositories on a quarterly basis;~~

~~(iii) identifying points of contact for roles and responsibilities relating to the implementation of this Act; and~~

~~(iv) if practicable, using existing procedures and systems; and~~

~~(B) corrects or amends any policies of the agency that are inconsistent with the requirements of this Act.~~

~~(2) FEDERAL CIO.—~~

~~(A) FRAMEWORK FOR REVIEW.—Not later than 1 year after the date of enactment of this Act, the Federal Chief Information Officer shall establish a framework for reviewing the software being developed across the Federal Government to surface and support the goals of existing digital priorities.~~

~~(B) MINIMUM STANDARD REPORTING REQUIREMENTS.—Not later than 120 days after the date of enactment of this Act, the Federal CIO shall, in coordination with the Director of the National Institute of Standards and Technology, establish minimum standard reporting requirements for the Chief Information Officers of agencies, which shall include information relating to—~~

~~(i) measuring the frequency of reuse of code, including access and modification;~~

~~(ii) whether the shared code is maintained;~~

~~(iii) whether there is a feedback mechanism for improvements to or community development of the shared code; and~~

~~(iv) the number and circumstances of all exemptions granted under section 5(b)(2).~~

~~(C) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Federal Chief Information Officer shall submit to Congress a report on the status of the implementation of this Act by each agency, including—~~

~~(i) a complete list of all exemptions granted under section 5(b)(2);~~

~~(ii) a table showing whether each agency has updated the acquisition and other policies of the agency to be compliant with this Act; and~~

~~(iii) an evaluation of the compliance of the agency with the framework described in subparagraph (A).~~

~~**SEC. 5. SCOPE AND APPLICABILITY.**~~

~~(a) NEW CUSTOM-DEVELOPED CODE ONLY.—This Act shall apply to custom-developed code that is developed or revised—~~

~~(1) by a Federal employee not less than 180 days after the date of enactment of this Act; or~~

~~(2) under a contract awarded pursuant to a solicitation issued not less than 180 days after the date of enactment of this Act.~~

~~(b) EXEMPTIONS.—~~

~~(1) AUTOMATIC.—This Act shall not apply to classified source code or source code developed primarily for use in a national security system, as defined in section 11103 of title 40, United States Code.~~

~~(2) EXPLANATION REQUIRED.—~~

~~(A) IN GENERAL.—The Chief Information Officer of an agency may exempt from the requirements of this Act any source code for which a limited exemption described in subparagraph (B) applies, after documenting the limited exemption and providing to the Federal Chief Information Officer a brief narrative justification, with redactions as appropriate.~~

~~(B) LIMITED EXEMPTIONS.—The limited exemptions described in this subparagraph are the following:~~

~~(i) The sharing or discovery of the source code is restricted by Federal law or regulation, including the Export Administration Regulations, the International Traffic in Arms Regulations, regulations of the Transportation Security Administration relating to the protection of Sensitive Security Information, and the Federal laws and regulations governing classified information.~~

~~(ii) The sharing or discovery of the source code would create an identifiable risk to individual privacy.~~

~~SEC. 6. GUIDANCE.~~

~~The Director of the Office of Management and Budget shall issue guidance, consistent with the purpose of this Act, that establishes best practices and uniform procedures across agencies under section 4(d).~~

~~SEC. 7. GAO REPORT ON INFORMATION TECHNOLOGY PRACTICES.~~

~~(a) INITIAL REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General~~

~~of the United States shall submit to Congress a report that includes an assessment of—~~

~~(1) duplicative software procurement across and within agencies, including estimates of the frequency, severity, and dollar value of the duplicative software procurement;~~

~~(2) barriers to agency use of cloud-based platforms for software development and version control and how to address those barriers;~~

~~(3) how source code sharing and open-source software collaboration can improve cybersecurity at agencies; and~~

~~(4) other relevant matters, as determined by the Comptroller General of the United States.~~

~~(b) SUPPLEMENTAL REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report that includes an assessment of—~~

~~(1) the implementation of this Act; and~~

~~(2) other relevant matters, as determined by the Comptroller General of the United States.~~

~~SEC. 8. RULE OF CONSTRUCTION.~~

~~Nothing in this Act shall be construed to require the disclosure of information or records that are exempt from public disclosure under section 552 of title 5, United~~

~~States Code (commonly known as the "Freedom of Information Act").~~

~~**SEC. 9. NO ADDITIONAL FUNDING.**~~

~~No additional funds are authorized to be appropriated to carry out this Act.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Source code Harmonization And Reuse in Information Technology Act" or the "SHARE IT Act".

SEC. 2. FINDINGS; PURPOSE.

(a) FINDINGS.—

(1) IN GENERAL.—Congress finds the following:

(A) DUPLICATION OF EFFORTS.—Federal agencies often engage in the development or procurement of similar software solutions for comparable problems, leading to a duplicative allocation of resources that could otherwise be avoided.

(B) COST INEFFICIENCY.—The absence of a mechanism for inter-agency source code sharing results in the Federal Government incurring unnecessary costs for software development, licensing, and maintenance, an inefficiency highlighted by the Government Accountability Office in numerous reports, including—

(i) Government Accountability Office Report "Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide" (GAO–14–413), published on May 22, 2014;

(ii) Government Accountability Office Report "2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits" (GAO–16–375SP), published on April 13, 2016;

(iii) Government Accountability Office Report "Information Technology: DoD Needs to Fully Implement Program for Piloting Open Source Software" (GAO–19–457), published on September 10, 2019;

(iv) Government Accountability Office Report "Information Technology: Federal Agencies and OMB Need to Continue to Improve Management and Cybersecurity" (GAO–20–691T), published on August 3, 2020; and

(v) Government Accountability Office Report "DoD Software Licenses: Better Guidance and Plans Needed to Ensure Re-

strictive Practices are Mitigated" (GAO–23–106290), published on September 12, 2023.

(C) TECHNOLOGICAL FRAGMENTATION.—The isolated development efforts of each agency contribute to a landscape of fragmented technologies that impede interoperability and data exchange between Federal systems.

(D) SLOW ADOPTION OF BEST PRACTICES.—The lack of software sharing hinders the diffusion of engineering best practices and innovations across agencies, whereas learning from the successes and failures of other agencies would accelerate the modernization of government systems.

(E) SECURITY VULNERABILITIES.—Redundant development efforts mean that security weaknesses inadvertently introduced in the software of an agency could go unnoticed by other agencies, whereas a shared codebase would benefit from collective security auditing and updates.

(F) PUBLIC ACCOUNTABILITY.—Software funded by taxpayers should be available for scru-

tiny by the public to the greatest extent possible, to ensure transparency and accountability.

(G) Pilot success.—Preliminary initiatives aimed at making federally funded custom-developed code freely available to the public have demonstrated the viability and benefits of such sharing schemes, including—

(i) Memorandum M–16–21 issued by the Office of Management and Budget on August 8, 2016, entitled "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software"; and

(ii) "Code.gov", which documents how agencies already extensively use public repositories, demonstrating the ability of agencies to share code using existing infrastructure.

(2) Conclusion.—Based on the findings in paragraph (1), it is imperative for Congress to enact legislation that mandates the sharing of custom-developed code across agencies to promote efficiency, reduce waste, enhance security, and foster innovation in the Federal information technology ecosystem.

(b) PURPOSE.—The overarching aim of this Act is to maximize efficiency, minimize duplication, and enhance security and innovation across Federal agencies by requiring the sharing of custom-developed code between agencies by—

(1) enabling agencies to benefit mutually from the investments of other agencies in custom-developed code;

(2) promoting technological consistency and interoperability among agencies, thereby facilitating seamless data exchange and system integration;

(3) fostering a culture of sharing engineering best practices and successful technological innovations among agencies;

(4) enhancing transparency by making federally funded custom-developed code available for public scrutiny, subject to necessary security considerations; and

(5) leveraging inter-agency collaboration for better security auditing of the shared codebase, aiming for a more unified and secure technological infrastructure across agencies.

SEC. 3. DEFINITIONS.

In this Act:

(1) Agency.—The term "agency" has the meaning given that term in section 3502 of title 44, United States Code.

(2) Appropriate congressional committees.—The term "appropriate congressional committees" means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Accountability of the House of Representatives.

(3) Custom-developed code.—The term "custom-developed code"—

(A) means source code that is—

(i) produced in the performance of a Federal contract or is otherwise exclusively funded by the Federal Government; or

(ii) developed by a Federal employee as part of the official duties of the employee;

(B) includes—

(i) source code, or segregable portions of source code, for which the Federal Government could obtain unlimited rights under part 27 of the Federal Acquisition Regulation or any relevant supplemental acquisition regulations of an agency; and

(ii) source code written for a software project, module, plugin, script, middleware, or application programming interface; and

(C) does not include—

(i) source code that is solely exploratory or disposable in nature, including source code written by a developer experimenting with a new language or library;

(ii) commercial computer software, commercial off-the-shelf software, or configuration scripts for such software; or

(iii) source code that is used in the performance of, but not produced in fulfillment of, a Federal contract.

(4) FEDERAL EMPLOYEE.—The term "Federal employee" has the meaning given the term "employee" in section 2105(a) of title 5, United States Code.

(5) METADATA.—The term "metadata", with respect to custom-developed code—

(A) has the meaning given that term in section 3502 of title 44, United States Code; and

(B) includes information on whether the custom-developed code—

(i) was produced pursuant to a contract, and the contract number, if any; and

(ii) is shared in a public or private repository, and includes a hyperlink to the repository, as applicable.

(6) PRIVATE REPOSITORY.—The term "private repository" means a software storage location—

(A) that contains source code, documentation, and other files; and

(B) access to which is restricted to authorized users.

(7) PUBLIC REPOSITORY.—The term "public repository" means a software storage location—

(A) that contains source code, documentation, and other files; and

(B) access to which is open to the public.

(8) SOFTWARE.—The term "software" has the meaning given the term "computer software" in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

(9) SOURCE CODE.—The term "source code" means a collection of computer commands written in a computer programming language that a computer can execute as a piece of software.

SEC. 4. SOFTWARE REUSE.

(a) SHARING.—Not later than 210 days after the date of enactment of this Act, the head of each agency shall ensure that—

(1) the custom-developed code of the agency is contained at not less than 1 public or private repository and is accessible to Federal employees via procedures developed under subsection (d)(1)(A)(ii)(III); and

(2) all software and other key technical components, including documentation, data models, schemas, metadata, and architecture designs, are owned by the agency.

(b) SOFTWARE REUSE RIGHTS IN PROCUREMENT CONTRACTS.—

(1) IN GENERAL.—The head of an agency that enters into a contract for the custom development of software shall acquire and enforce rights sufficient to enable the governmentwide access, execution, and modification of the custom-developed code relating to the software.

(2) BEST PRACTICES.—

(A) CONTRACT ADMINISTRATION.—With respect to a contract described in paragraph (1), the head of an agency shall ensure appropriate contract administration and use of best practices

to secure the full scope of licenses and rights for the Federal Government of the custom-developed code developed under the contract, to allow for access, execution, and modification by other agencies.

(B) DEVELOPMENT PROCESS.—With respect to a contract described in paragraph (1), the head of an agency shall ensure the use of best practices to require and obtain the delivery of the custom-developed code, documentation of the custom-developed code, configuration and artifacts required to develop, build, test, and deploy the custom-developed code, and other associated materials from the developer throughout the development process.

(c) DISCOVERY.—Not later than 210 days after the date of enactment of this Act, the head of each agency shall make metadata for the custom-developed code of the agency publicly accessible.

(d) ACCOUNTABILITY MECHANISMS.—

(1) AGENCY CIOS.—Not later than 180 days after the date of enactment of this Act, the Chief Information Officer of each agency, in consultation with the Chief Acquisition Officer, or similar official, of the agency and the Administrator of the Office of Elec-

tronic Government, shall develop an agency-wide policy that—

(A) addresses the requirements of this Act, including—

(i) ensuring that agency custom-developed code follows best practices for operating repositories and version control systems to keep track of changes and to facilitate collaboration among multiple developers;

(ii) managing the sharing and discovery of source code, including developing—

(I) procedures to determine whether any custom-developed code meets the conditions for an exemption under this Act;

(II) procedures for making metadata for custom-developed code discoverable, pursuant to subsection (c);

(III) procedures for Federal employees to discover and gain access to private repositories;

(IV) procedures for checking the use of existing shared code as an alternative to initiating a new project or procurement;

(V) standardized reporting practices across the agency to capture key information relating to a contract for reporting statistics about the contract; and

(VI) procedures for updating metadata, private repositories, and public repositories on a quarterly basis;

(iii) identifying points of contact for roles and responsibilities relating to the implementation of this Act; and

(iv) if practicable, using existing procedures and systems; and

(B) corrects or amends any policies of the agency that are inconsistent with the requirements of this Act.

(2) ADMINISTRATOR OF THE OFFICE OF ELECTRONIC GOVERNMENT.—

(A) FRAMEWORK FOR REVIEW.—Not later than 1 year after the date of enactment of this

Act, the Administrator of the Office of Electronic Government shall establish a framework for reviewing the software being developed across the Federal Government to surface and support the goals of existing digital priorities, including issuing guidance on—

(i) the implementation of subsection (c);

(ii) websites for agencies to use with respect to code discovery under subsection (c);

(iii) other procedures for agencies to use to ensure that existing shared code has been considered as an alternative to initiating a new project or procurement;

(iv) identifying exemptions to this Act; and

(v) the frequency of and official responsible for security auditing of repositories.

(B) MINIMUM STANDARD REPORTING REQUIREMENTS.—Not later than 120 days after the date of enactment of this Act, the Administrator of the Office of Electronic Government, in coordination with the Director of the National Institute of Standards and Technology, shall establish

minimum standard reporting requirements for the Chief Information Officers of agencies, which shall include information relating to—

(i) measuring the frequency of reuse of code, including access and modification;

(ii) whether the shared code is maintained;

(iii) whether there is a feedback mechanism for improvements to or community development of the shared code; and

(iv) the number and circumstances of all exemptions granted under section 5(b)(2).

SEC. 5. SCOPE AND APPLICABILITY.

(a) NEW CUSTOM-DEVELOPED CODE ONLY.—The requirements under section 4 shall apply to custom-developed code that is developed or revised—

(1) by a Federal employee not less than 180 days after the date of enactment of this Act; or

(2) under a contract awarded pursuant to a solicitation issued not less than 180 days after the date of enactment of this Act.

(b) EXEMPTIONS.—

(1) AUTOMATIC.—

(A) National security.—An exemption from the requirements under section 4 shall apply to classified source code or source code developed—

(i) primarily for use in a national security system, as defined in section 11103 of title 40, United States Code; or

(ii) by an agency, or part of an agency, that is an element of the intelligence community, as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(B) Freedom of information act.—An exemption from the requirements under section 4 shall apply to source code the disclosure of which is exempt under section 552(b) of title 5, United States Code (commonly known as the "Freedom of Information Act").

(2) Discretionary.—

(A) Exemptions and guidance.—

(i) In general.—The Chief Information Officer of an agency, in consultation with the Federal Privacy Council, or any successor thereto, may exempt from the requirements of section 4 any source code for

which a limited exemption described in subparagraph (B) applies.

(ii) GUIDANCE REQUIRED.—The Federal Privacy Council shall provide guidance to the Chief Information Officer of each agency relating to the limited exemption described in subparagraph (B)(ii) to ensure consistent application of this paragraph across agencies.

(B) LIMITED EXEMPTIONS.—The limited exemptions described in this subparagraph are the following:

(i) The sharing or discovery of the source code is restricted by Federal law or regulation, including the Export Administration Regulations, the International Traffic in Arms Regulations, regulations of the Transportation Security Administration relating to the protection of Sensitive Security Information, and the Federal laws and regulations governing classified information.

(ii) The sharing or discovery of the source code would create an identifiable risk to individual privacy.

(3) REPORTS REQUIRED.—

(A) IN GENERAL.—Not later than December 31 of each year, the Chief Information Officer of an agency shall submit to the Administrator of the Office of Electronic Government a report of the source code of the agency to which an exemption under paragraph (1) or (2) applied during the fiscal year ending on September 30 of that year with a brief narrative justification of each exemption.

(B) FORM.—The report under subparagraph (A) shall be submitted in unclassified form, with a classified annex as appropriate.

(C) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Administrator of the Office of Electronic Government shall submit to the appropriate congressional committees a report on the status of the implementation of this Act by each agency, including—

(i) a compilation of all information, including a narrative justification, relating to each exemption granted under paragraph (1) or (2);

(ii) a table showing whether each agency has updated the acquisition and other policies of the agency to be compliant with this Act;

(iii) an evaluation of the compliance of the agency with the framework described in section 4(d)(2)(A); and

(iv) a classified annex as appropriate.

SEC. 6. GUIDANCE.

The Director of the Office of Management and Budget shall issue guidance, consistent with the purpose of this Act, that establishes best practices and uniform procedures across agencies under section 4(d).

SEC. 7. GAO REPORT ON INFORMATION TECHNOLOGY PRACTICES.

(a) INITIAL REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes an assessment of—

(1) duplicative software procurement across and within agencies, including estimates of the frequency, severity, and dollar value of the duplicative software procurement;

(2) barriers to agency use of cloud-based platforms for software development and version control and how to address those barriers;

(3) how source code sharing and open-source software collaboration can improve cybersecurity at agencies; and

(4) other relevant matters, as determined by the Comptroller General of the United States.

(b) SUPPLEMENTAL REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes an assessment of—

(1) the implementation of this Act; and

(2) other relevant matters, as determined by the Comptroller General of the United States.

SEC. 8. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed to require the disclosure of information or records that are exempt from public disclosure under section 552 of title 5, United States Code (commonly known as the "Freedom of Information Act").

SEC. 9. NO ADDITIONAL FUNDING.

No additional funds are authorized to be appropriated to carry out this Act.

SEC. 10. GAO REPORT ON EFFECTIVENESS.

Not later than 540 days after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the effectiveness of this Act.

Calendar No. 491

118TH CONGRESS
2D SESSION

S. 3594

[Report No. 118–213]

A BILL

To require governmentwide source code sharing, and for other purposes.

SEPTEMBER 9, 2024

Reported with an amendment