

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Source code Harmoni-
5 zation And Reuse in Information Technology Act” or the
6 “SHARE IT Act”.

1 **SEC. 2. FINDINGS; PURPOSE.**

2 (a) FINDINGS.—

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

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

10 (B) COST INEFFICIENCY.—The absence of
11 a mechanism for inter-agency source code shar-
12 ing results in the Federal Government incurring
13 unnecessary costs for software development, li-
14 censing, and maintenance, an inefficiency high-
15 lighted by the Government Accountability Office
16 in numerous reports, including—

17 (i) Government Accountability Office
18 Report “Federal Software Licenses: Better
19 Management Needed to Achieve Signifi-
20 cant Savings Government-Wide” (GAO-
21 14-413), published on May 22, 2014;

22 (ii) Government Accountability Office
23 Report “2016 Annual Report: Additional
24 Opportunities to Reduce Fragmentation,
25 Overlap, and Duplication and Achieve

1 Other Financial Benefits” (GAO-16-
2 375SP), published on April 13, 2016;

3 (iii) Government Accountability Office
4 Report “Information Technology: DoD
5 Needs to Fully Implement Program for Pi-
6 loting Open Source Software” (GAO-19-
7 457), published on September 10, 2019;

8 (iv) Government Accountability Office
9 Report “Information Technology: Federal
10 Agencies and OMB Need to Continue to
11 Improve Management and Cybersecurity”
12 (GAO-20-691T), published on August 3,
13 2020; and

14 (v) Government Accountability Office
15 Report “DoD Software Licenses: Better
16 Guidance and Plans Needed to Ensure Re-
17 strictive Practices are Mitigated” (GAO-
18 23-106290), published on September 12,
19 2023.

20 (C) TECHNOLOGICAL FRAGMENTATION.—

21 The isolated development efforts of each agency
22 contribute to a landscape of fragmented tech-
23 nologies that impede interoperability and data
24 exchange between Federal systems.

1 (D) SLOW ADOPTION OF BEST PRAC-
2 TICES.—The lack of software sharing hinders
3 the diffusion of engineering best practices and
4 innovations across agencies, whereas learning
5 from the successes and failures of other agen-
6 cies would accelerate the modernization of gov-
7 ernment systems.

8 (E) SECURITY VULNERABILITIES.—Redun-
9 dant development efforts mean that security
10 weaknesses inadvertently introduced in the soft-
11 ware of an agency could go unnoticed by other
12 agencies, whereas a shared codebase would ben-
13 efit from collective security auditing and up-
14 dates.

15 (F) PUBLIC ACCOUNTABILITY.—Software
16 funded by taxpayers should be available for
17 scrutiny by the public to the greatest extent
18 possible, to ensure transparency and account-
19 ability.

20 (G) PILOT SUCCESS.—Preliminary initia-
21 tives aimed at making federally funded custom-
22 developed code freely available to the public
23 have demonstrated the viability and benefits of
24 such sharing schemes, including—

1 (i) Memorandum M-16-21 issued by
2 the Office of Management and Budget on
3 August 8, 2016, entitled “Federal Source
4 Code Policy: Achieving Efficiency, Trans-
5 parency, and Innovation through Reusable
6 and Open Source Software”; and

7 (ii) “Code.gov”, which documents how
8 agencies already extensively use public re-
9 positories, demonstrating the ability of
10 agencies to share code using existing infra-
11 structure.

12 (2) CONCLUSION.—Based on the findings in
13 paragraph (1), it is imperative for Congress to enact
14 legislation that mandates the sharing of custom-de-
15 veloped code across agencies to promote efficiency,
16 reduce waste, enhance security, and foster innova-
17 tion in the Federal information technology eco-
18 system.

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

1 (1) enabling agencies to benefit mutually from
2 the investments of other agencies in custom-devel-
3 oped code;

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

7 (3) fostering a culture of sharing engineering
8 best practices and successful technological innova-
9 tions among agencies;

10 (4) enhancing transparency by making federally
11 funded custom-developed code available for public
12 scrutiny, subject to necessary security consider-
13 ations; and

14 (5) leveraging inter-agency collaboration for
15 better security auditing of the shared codebase, aim-
16 ing for a more unified and secure technological in-
17 frastructure across agencies.

18 **SEC. 3. DEFINITIONS.**

19 In this Act:

20 (1) **AGENCY.**—The term “agency” has the
21 meaning given that term in section 3502 of title 44,
22 United States Code.

23 (2) **CUSTOM-DEVELOPED CODE.**—The term
24 “custom-developed code”—

25 (A) means source code that is—

1 (i) produced in the performance of a
 2 Federal contract or is otherwise fully fund-
 3 ed by the Federal Government; or

4 (ii) developed by a Federal employee
 5 as part of the official duties of the em-
 6 ployee;

7 ~~(B)~~ includes—

8 (i) source code, or segregable portions
 9 of source code, for which the Federal Gov-
 10 ernment could obtain unlimited rights
 11 under part 27 of the Federal Acquisition
 12 Regulation or any relevant supplemental
 13 acquisition regulations of an agency; and

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

17 ~~(C)~~ does not include—

18 (i) source code that is solely explor-
 19 atory or disposable in nature, including
 20 source code written by a developer experi-
 21 menting with a new language or library; or

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

24 ~~(3)~~ FEDERAL CHIEF INFORMATION OFFICER.—

25 The term “Federal Chief Information Officer”

1 means the Administrator of the Office of Electronic
2 Government.

3 (4) ~~FEDERAL EMPLOYEE.~~—The term “Federal
4 employee” has the meaning given the term “em-
5 ployee” in section 2105(a) of title 5, United States
6 Code.

7 (5) ~~METADATA.~~—The term “metadata”, with
8 respect to custom-developed code—

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

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

14 (i) was produced pursuant to a con-
15 tract, and the contract number, if any; and

16 (ii) is shared in a public or private re-
17 pository, and includes a hyperlink to the
18 repository, as applicable.

19 (6) ~~PRIVATE REPOSITORY.~~—The term “private
20 repository” means a software storage location—

21 (A) that contains source code, documenta-
22 tion, and other files; and

23 (B) access to which is restricted to author-
24 ized users.

1 (7) PUBLIC REPOSITORY.—The term “public
2 repository” means a software storage location—

3 (A) that contains source code, documenta-
4 tion, and other files; and

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

6 (8) SOFTWARE.—The term “software” has the
7 meaning given the term “computer software” in sec-
8 tion 2.101 of title 48, Code of Federal Regulations,
9 or any successor regulation.

10 (9) SOURCE CODE.—The term “source code”
11 means a collection of computer commands written in
12 a computer programming language that a computer
13 can execute as a piece of software.

14 **SEC. 4. SOFTWARE REUSE.**

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

18 (1) the custom-developed code of the agency is
19 contained at not less than 1 public or private reposi-
20 tory and is accessible to Federal employees via pro-
21 cedures developed under subsection
22 (d)(1)(A)(ii)(III); and

23 (2) all software and other key technical compo-
24 nents, including documentation, data models,

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

3 (b) SOFTWARE REUSE RIGHTS IN PROCUREMENT
4 CONTRACTS.—

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

11 (2) BEST PRACTICES.—

12 (A) CONTRACT ADMINISTRATION.—With
13 respect to a contract described in paragraph
14 (1), the head of an agency shall ensure appro-
15 priate contract administration and use of best
16 practices to secure the full scope of licenses and
17 rights for the Federal Government of the cus-
18 tom-developed code developed under the con-
19 tract, to allow for access, execution, and modi-
20 fication by other agencies.

21 (B) DEVELOPMENT PROCESS.—With re-
22 spect to a contract described in paragraph (1),
23 the head of an agency shall ensure the use of
24 best practices to require and obtain the delivery
25 of the custom-developed code, documentation of

1 the custom-developed code, configuration and
2 artifacts required to develop, build, test, and
3 deploy the custom-developed code, and other as-
4 sociated materials from the developer through-
5 out the development process.

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

10 (d) ACCOUNTABILITY MECHANISMS.—

11 (1) AGENCY CIOS.—Not later than 180 days
12 after the date of enactment of this Act, the Chief In-
13 formation Officer of each agency, in consultation
14 with the Chief Acquisition Officer, or similar official,
15 of the agency and the Federal Chief Information Of-
16 ficer, shall develop an agency-wide policy that—

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

19 (i) ensuring that agency custom-devel-
20 oped code follows best practices for oper-
21 ating repositories and version control sys-
22 tems to keep track of changes and to facili-
23 tate collaboration among multiple devel-
24 opers;

1 (ii) managing the sharing and dis-
2 ecovery of source code, including devel-
3 oping—

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

8 (II) procedures for making
9 metadata for custom-developed code
10 discoverable, pursuant to section 4(e);

11 (III) procedures for Federal em-
12 ployees to discover and gain access to
13 private repositories;

14 (IV) standardized reporting prac-
15 tices across the agency to capture key
16 information relating to a contract for
17 reporting statistics about the contract;
18 and

19 (V) procedures for updating
20 metadata, private repositories, and
21 public repositories on a quarterly
22 basis;

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

1 (iv) if practicable, using existing pro-
2 cedures and systems; and

3 (B) corrects or amends any policies of the
4 agency that are inconsistent with the require-
5 ments of this Act.

6 (2) FEDERAL CIO.—

7 (A) FRAMEWORK FOR REVIEW.—Not later
8 than 1 year after the date of enactment of this
9 Act, the Federal Chief Information Officer shall
10 establish a framework for reviewing the soft-
11 ware being developed across the Federal Gov-
12 ernment to surface and support the goals of ex-
13 isting digital priorities.

14 (B) MINIMUM STANDARD REPORTING RE-
15 QUIREMENTS.—Not later than 120 days after
16 the date of enactment of this Act, the Federal
17 CIO shall, in coordination with the Director of
18 the National Institute of Standards and Tech-
19 nology, establish minimum standard reporting
20 requirements for the Chief Information Officers
21 of agencies, which shall include information re-
22 lating to—

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

1 (ii) whether the shared code is main-
2 tained;

3 (iii) whether there is a feedback mech-
4 anism for improvements to or community
5 development of the shared code; and

6 (iv) the number and circumstances of
7 all exemptions granted under section
8 5(b)(2).

9 (C) ANNUAL REPORT.—Not later than 1
10 year after the date of enactment of this Act,
11 and annually thereafter, the Federal Chief In-
12 formation Officer shall submit to Congress a re-
13 port on the status of the implementation of this
14 Act by each agency, including—

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

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

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

1 **SEC. 5. SCOPE AND APPLICABILITY.**

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

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

7 (2) under a contract awarded pursuant to a so-
8 licitation issued not less than 180 days after the
9 date of enactment of this Act.

10 (b) ~~EXEMPTIONS.~~—

11 (1) ~~AUTOMATIC.~~—This Act shall not apply to
12 classified source code or source code developed pri-
13 marily for use in a national security system, as de-
14 fined in section 11103 of title 40, United States
15 Code.

16 (2) ~~EXPLANATION REQUIRED.~~—

17 (A) ~~IN GENERAL.~~—The Chief Information
18 Officer of an agency may exempt from the re-
19 quirements of this Act any source code for
20 which a limited exemption described in subpara-
21 graph (B) applies, after documenting the lim-
22 ited exemption and providing to the Federal
23 Chief Information Officer a brief narrative jus-
24 tification, with redactions as appropriate.

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

4 (i) The sharing or discovery of the
5 source code is restricted by Federal law or
6 regulation, including the Export Adminis-
7 tration Regulations, the International
8 Traffic in Arms Regulations, regulations of
9 the Transportation Security Administra-
10 tion relating to the protection of Sensitive
11 Security Information, and the Federal laws
12 and regulations governing classified infor-
13 mation.

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

17 **SEC. 6. GUIDANCE.**

18 The Director of the Office of Management and Budget
19 shall issue guidance, consistent with the purpose of this
20 Act, that establishes best practices and uniform proce-
21 dures across agencies under section 4(d).

22 **SEC. 7. GAO REPORT ON INFORMATION TECHNOLOGY**
23 **PRACTICES.**

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

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

3 (1) duplicative software procurement across and
4 within agencies, including estimates of the fre-
5 quency, severity, and dollar value of the duplicative
6 software procurement;

7 (2) barriers to agency use of cloud-based plat-
8 forms for software development and version control
9 and how to address those barriers;

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

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

15 (b) SUPPLEMENTAL REPORT.—Not later than 2
16 years after the date of enactment of this Act, the Comp-
17 troller General of the United States shall submit to Con-
18 gress a report that includes an assessment of—

19 (1) the implementation of this Act; and

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

22 **SEC. 8. RULE OF CONSTRUCTION.**

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

1 States Code (commonly known as the “Freedom of Infor-
2 mation Act”).

3 **SEC. 9. NO ADDITIONAL FUNDING.**

4 No additional funds are authorized to be appro-
5 priated to carry out this Act.

6 **SECTION 1. SHORT TITLE.**

7 *This Act may be cited as the “Source code Harmoni-
8 zation And Reuse in Information Technology Act” or the
9 “SHARE IT Act”.*

10 **SEC. 2. FINDINGS; PURPOSE.**

11 *(a) FINDINGS.—*

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

13 *(A) DUPLICATION OF EFFORTS.—Federal*
14 *agencies often engage in the development or pro-*
15 *curement of similar software solutions for com-*
16 *parable problems, leading to a duplicative allo-*
17 *cation of resources that could otherwise be avoid-*
18 *ed.*

19 *(B) COST INEFFICIENCY.—The absence of a*
20 *mechanism for inter-agency source code sharing*
21 *results in the Federal Government incurring un-*
22 *necessary costs for software development, licens-*
23 *ing, and maintenance, an inefficiency high-*
24 *lighted by the Government Accountability Office*
25 *in numerous reports, including—*

1 (i) *Government Accountability Office*
2 *Report “Federal Software Licenses: Better*
3 *Management Needed to Achieve Significant*
4 *Savings Government-Wide” (GAO–14–413),*
5 *published on May 22, 2014;*

6 (ii) *Government Accountability Office*
7 *Report “2016 Annual Report: Additional*
8 *Opportunities to Reduce Fragmentation,*
9 *Overlap, and Duplication and Achieve*
10 *Other Financial Benefits” (GAO–16–*
11 *375SP), published on April 13, 2016;*

12 (iii) *Government Accountability Office*
13 *Report “Information Technology: DoD*
14 *Needs to Fully Implement Program for Pi-*
15 *loting Open Source Software” (GAO–19–*
16 *457), published on September 10, 2019;*

17 (iv) *Government Accountability Office*
18 *Report “Information Technology: Federal*
19 *Agencies and OMB Need to Continue to Im-*
20 *prove Management and Cybersecurity”*
21 *(GAO–20–691T), published on August 3,*
22 *2020; and*

23 (v) *Government Accountability Office*
24 *Report “DoD Software Licenses: Better*
25 *Guidance and Plans Needed to Ensure Re-*

1 *strictive Practices are Mitigated” (GAO–*
2 *23–106290), published on September 12,*
3 *2023.*

4 (C) *TECHNOLOGICAL FRAGMENTATION.—*
5 *The isolated development efforts of each agency*
6 *contribute to a landscape of fragmented tech-*
7 *nologies that impede interoperability and data*
8 *exchange between Federal systems.*

9 (D) *SLOW ADOPTION OF BEST PRACTICES.—*
10 *The lack of software sharing hinders the diffu-*
11 *sion of engineering best practices and innova-*
12 *tions across agencies, whereas learning from the*
13 *successes and failures of other agencies would ac-*
14 *celerate the modernization of government sys-*
15 *tems.*

16 (E) *SECURITY VULNERABILITIES.—Redun-*
17 *dant development efforts mean that security*
18 *weaknesses inadvertently introduced in the soft-*
19 *ware of an agency could go unnoticed by other*
20 *agencies, whereas a shared codebase would ben-*
21 *efit from collective security auditing and up-*
22 *dates.*

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

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

3 (G) *PILOT SUCCESS.*—*Preliminary initia-*
4 *tives aimed at making federally funded custom-*
5 *developed code freely available to the public have*
6 *demonstrated the viability and benefits of such*
7 *sharing schemes, including—*

8 (i) *Memorandum M–16–21 issued by*
9 *the Office of Management and Budget on*
10 *August 8, 2016, entitled “Federal Source*
11 *Code Policy: Achieving Efficiency, Trans-*
12 *parency, and Innovation through Reusable*
13 *and Open Source Software”; and*

14 (ii) *“Code.gov”, which documents how*
15 *agencies already extensively use public re-*
16 *positories, demonstrating the ability of*
17 *agencies to share code using existing infra-*
18 *structure.*

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

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

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

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

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

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

18 (5) *leveraging inter-agency collaboration for bet-*
19 *ter security auditing of the shared codebase, aiming*
20 *for a more unified and secure technological infra-*
21 *structure across agencies.*

22 **SEC. 3. DEFINITIONS.**

23 *In this Act:*

1 (1) *AGENCY.*—*The term “agency” has the mean-*
2 *ing given that term in section 3502 of title 44, United*
3 *States Code.*

4 (2) *APPROPRIATE CONGRESSIONAL COMMIT-*
5 *TEES.*—*The term “appropriate congressional commit-*
6 *tees” means the Committee on Homeland Security*
7 *and Governmental Affairs of the Senate and the Com-*
8 *mittee on Oversight and Accountability of the House*
9 *of Representatives.*

10 (3) *CUSTOM-DEVELOPED CODE.*—*The term “cus-*
11 *tom-developed code”—*

12 (A) *means source code that is—*

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

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

18 (B) *includes—*

19 (i) *source code, or segregable portions*
20 *of source code, for which the Federal Gov-*
21 *ernment could obtain unlimited rights*
22 *under part 27 of the Federal Acquisition*
23 *Regulation or any relevant supplemental*
24 *acquisition regulations of an agency; and*

1 (ii) source code written for a software
2 project, module, plugin, script, middleware,
3 or application programming interface; and
4 (C) does not include—

5 (i) source code that is solely explor-
6 atory or disposable in nature, including
7 source code written by a developer experi-
8 menting with a new language or library;

9 (ii) commercial computer software,
10 commercial off-the-shelf software, or configu-
11 ration scripts for such software; or

12 (iii) source code that is used in the
13 performance of, but not produced in fulfill-
14 ment of, a Federal contract.

15 (4) *FEDERAL EMPLOYEE.*—The term “Federal
16 employee” has the meaning given the term “em-
17 ployee” in section 2105(a) of title 5, United States
18 Code.

19 (5) *METADATA.*—The term “metadata”, with re-
20 spect to custom-developed code—

21 (A) has the meaning given that term in sec-
22 tion 3502 of title 44, United States Code; and

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

1 (i) was produced pursuant to a con-
2 tract, and the contract number, if any; and

3 (ii) is shared in a public or private re-
4 pository, and includes a hyperlink to the re-
5 pository, as applicable.

6 (6) *PRIVATE REPOSITORY*.—The term “private
7 repository” means a software storage location—

8 (A) that contains source code, documenta-
9 tion, and other files; and

10 (B) access to which is restricted to author-
11 ized users.

12 (7) *PUBLIC REPOSITORY*.—The term “public re-
13 pository” means a software storage location—

14 (A) that contains source code, documenta-
15 tion, and other files; and

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

17 (8) *SOFTWARE*.—The term “software” has the
18 meaning given the term “computer software” in sec-
19 tion 2.101 of title 48, Code of Federal Regulations, or
20 any successor regulation.

21 (9) *SOURCE CODE*.—The term “source code”
22 means a collection of computer commands written in
23 a computer programming language that a computer
24 can execute as a piece of software.

1 **SEC. 4. SOFTWARE REUSE.**

2 (a) *SHARING.*—Not later than 210 days after the date
3 of enactment of this Act, the head of each agency shall en-
4 sure that—

5 (1) *the custom-developed code of the agency is*
6 *contained at not less than 1 public or private reposi-*
7 *tory and is accessible to Federal employees via proce-*
8 *dures developed under subsection (d)(1)(A)(ii)(III);*
9 *and*

10 (2) *all software and other key technical compo-*
11 *nents, including documentation, data models,*
12 *schemas, metadata, and architecture designs, are*
13 *owned by the agency.*

14 (b) *SOFTWARE REUSE RIGHTS IN PROCUREMENT*
15 *CONTRACTS.*—

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

22 (2) *BEST PRACTICES.*—

23 (A) *CONTRACT ADMINISTRATION.*—*With re-*
24 *spect to a contract described in paragraph (1),*
25 *the head of an agency shall ensure appropriate*
26 *contract administration and use of best practices*

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

6 (B) *DEVELOPMENT PROCESS.*—With respect
7 to a contract described in paragraph (1), the
8 head of an agency shall ensure the use of best
9 practices to require and obtain the delivery of
10 the custom-developed code, documentation of the
11 custom-developed code, configuration and arti-
12 facts required to develop, build, test, and deploy
13 the custom-developed code, and other associated
14 materials from the developer throughout the de-
15 velopment process.

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

20 (d) *ACCOUNTABILITY MECHANISMS.*—

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

1 *tronic Government, shall develop an agency-wide pol-*
2 *icy that—*

3 *(A) addresses the requirements of this Act,*

4 *including—*

5 *(i) ensuring that agency custom-devel-*
6 *oped code follows best practices for oper-*
7 *ating repositories and version control sys-*
8 *tems to keep track of changes and to facili-*
9 *tate collaboration among multiple devel-*
10 *opers;*

11 *(ii) managing the sharing and dis-*
12 *covery of source code, including devel-*
13 *oping—*

14 *(I) procedures to determine wheth-*
15 *er any custom-developed code meets the*
16 *conditions for an exemption under this*
17 *Act;*

18 *(II) procedures for making*
19 *metadata for custom-developed code*
20 *discoverable, pursuant to subsection*
21 *(c);*

22 *(III) procedures for Federal em-*
23 *ployees to discover and gain access to*
24 *private repositories;*

1 (IV) *procedures for checking the*
2 *use of existing shared code as an alter-*
3 *native to initiating a new project or*
4 *procurement;*

5 (V) *standardized reporting prac-*
6 *tices across the agency to capture key*
7 *information relating to a contract for*
8 *reporting statistics about the contract;*
9 *and*

10 (VI) *procedures for updating*
11 *metadata, private repositories, and*
12 *public repositories on a quarterly*
13 *basis;*

14 (iii) *identifying points of contact for*
15 *roles and responsibilities relating to the im-*
16 *plementation of this Act; and*

17 (iv) *if practicable, using existing pro-*
18 *cedures and systems; and*

19 (B) *corrects or amends any policies of the*
20 *agency that are inconsistent with the require-*
21 *ments of this Act.*

22 (2) *ADMINISTRATOR OF THE OFFICE OF ELEC-*
23 *TRONIC GOVERNMENT.—*

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

1 *Act, the Administrator of the Office of Electronic*
2 *Government shall establish a framework for re-*
3 *viewing the software being developed across the*
4 *Federal Government to surface and support the*
5 *goals of existing digital priorities, including*
6 *issuing guidance on—*

7 *(i) the implementation of subsection*
8 *(c);*

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

12 *(iii) other procedures for agencies to*
13 *use to ensure that existing shared code has*
14 *been considered as an alternative to initi-*
15 *ating a new project or procurement;*

16 *(iv) identifying exemptions to this Act;*
17 *and*

18 *(v) the frequency of and official respon-*
19 *sible for security auditing of repositories.*

20 *(B) MINIMUM STANDARD REPORTING RE-*
21 *QUIREMENTS.—Not later than 120 days after the*
22 *date of enactment of this Act, the Administrator*
23 *of the Office of Electronic Government, in coordi-*
24 *nation with the Director of the National Insti-*
25 *tute of Standards and Technology, shall establish*

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

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

6 *(ii) whether the shared code is main-*
7 *tained;*

8 *(iii) whether there is a feedback mecha-*
9 *nism for improvements to or community de-*
10 *velopment of the shared code; and*

11 *(iv) the number and circumstances of*
12 *all exemptions granted under section*
13 *5(b)(2).*

14 **SEC. 5. SCOPE AND APPLICABILITY.**

15 *(a) NEW CUSTOM-DEVELOPED CODE ONLY.—The re-*
16 *quirements under section 4 shall apply to custom-developed*
17 *code that is developed or revised—*

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

20 *(2) under a contract awarded pursuant to a so-*
21 *licitation issued not less than 180 days after the date*
22 *of enactment of this Act.*

23 *(b) EXEMPTIONS.—*

24 *(1) AUTOMATIC.—*

1 (A) *NATIONAL SECURITY.*—An exemption
2 from the requirements under section 4 shall
3 apply to classified source code or source code de-
4 veloped—

5 (i) primarily for use in a national se-
6 curity system, as defined in section 11103
7 of title 40, United States Code; or

8 (ii) by an agency, or part of an agen-
9 cy, that is an element of the intelligence
10 community, as defined in section 3(4) of the
11 National Security Act of 1947 (50 U.S.C.
12 3003(4)).

13 (B) *FREEDOM OF INFORMATION ACT.*—An
14 exemption from the requirements under section 4
15 shall apply to source code the disclosure of which
16 is exempt under section 552(b) of title 5, United
17 States Code (commonly known as the “Freedom
18 of Information Act”).

19 (2) *DISCRETIONARY.*—

20 (A) *EXEMPTIONS AND GUIDANCE.*—

21 (i) *IN GENERAL.*—The Chief Informa-
22 tion Officer of an agency, in consultation
23 with the Federal Privacy Council, or any
24 successor thereto, may exempt from the re-
25 quirements of section 4 any source code for

1 *which a limited exemption described in sub-*
2 *paragraph (B) applies.*

3 *(ii) GUIDANCE REQUIRED.—The Fed-*
4 *eral Privacy Council shall provide guidance*
5 *to the Chief Information Officer of each*
6 *agency relating to the limited exemption de-*
7 *scribed in subparagraph (B)(ii) to ensure*
8 *consistent application of this paragraph*
9 *across agencies.*

10 *(B) LIMITED EXEMPTIONS.—The limited ex-*
11 *emptions described in this subparagraph are the*
12 *following:*

13 *(i) The sharing or discovery of the*
14 *source code is restricted by Federal law or*
15 *regulation, including the Export Adminis-*
16 *tration Regulations, the International Traf-*
17 *fic in Arms Regulations, regulations of the*
18 *Transportation Security Administration re-*
19 *lating to the protection of Sensitive Secu-*
20 *rity Information, and the Federal laws and*
21 *regulations governing classified informa-*
22 *tion.*

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

1 (3) *REPORTS REQUIRED.*—

2 (A) *IN GENERAL.*—Not later than December
3 31 of each year, the Chief Information Officer of
4 an agency shall submit to the Administrator of
5 the Office of Electronic Government a report of
6 the source code of the agency to which an exemp-
7 tion under paragraph (1) or (2) applied during
8 the fiscal year ending on September 30 of that
9 year with a brief narrative justification of each
10 exemption.

11 (B) *FORM.*—The report under subpara-
12 graph (A) shall be submitted in unclassified
13 form, with a classified annex as appropriate.

14 (C) *ANNUAL REPORT.*—Not later than 1
15 year after the date of enactment of this Act, and
16 annually thereafter, the Administrator of the Of-
17 fice of Electronic Government shall submit to the
18 appropriate congressional committees a report
19 on the status of the implementation of this Act
20 by each agency, including—

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

1 (ii) a table showing whether each agen-
2 cy has updated the acquisition and other
3 policies of the agency to be compliant with
4 this Act;

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

8 (iv) a classified annex as appropriate.

9 **SEC. 6. GUIDANCE.**

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

14 **SEC. 7. GAO REPORT ON INFORMATION TECHNOLOGY**
15 **PRACTICES.**

16 (a) *INITIAL REPORT.*—*Not later than 1 year after the*
17 *date of enactment of this Act, the Comptroller General of*
18 *the United States shall submit to the appropriate congres-*
19 *sional committees a report that includes an assessment of—*

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

1 (2) *barriers to agency use of cloud-based plat-*
2 *forms for software development and version control*
3 *and how to address those barriers;*

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

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

9 (b) *SUPPLEMENTAL REPORT.*—*Not later than 2 years*
10 *after the date of enactment of this Act, the Comptroller Gen-*
11 *eral of the United States shall submit to the appropriate*
12 *congressional committees a report that includes an assess-*
13 *ment of—*

14 (1) *the implementation of this Act; and*

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

17 **SEC. 8. RULE OF CONSTRUCTION.**

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

23 **SEC. 9. NO ADDITIONAL FUNDING.**

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

1 **SEC. 10. GAO REPORT ON EFFECTIVENESS.**

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

Calendar No. 491

118TH CONGRESS
2^D 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