

118TH CONGRESS  
2D SESSION

**S.** \_\_\_\_\_

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

---

IN THE SENATE OF THE UNITED STATES

---

Mr. CRUZ (for himself and Mr. PETERS) introduced the following bill; which was read twice and referred to the Committee on \_\_\_\_\_

---

**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”.

7 **SEC. 2. FINDINGS; PURPOSE.**

8 (a) FINDINGS.—

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

10 (A) DUPLICATION OF EFFORTS.—Federal  
11 agencies often engage in the development or

1 procurement of similar software solutions for  
2 comparable problems, leading to a duplicative  
3 allocation of resources that could otherwise be  
4 avoided.

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

12 (i) Government Accountability Office  
13 Report “Federal Software Licenses: Better  
14 Management Needed to Achieve Signifi-  
15 cant Savings Government-Wide” (GAO-14-  
16 413), published on May 22, 2014;

17 (ii) Government Accountability Office  
18 Report “2016 Annual Report: Additional  
19 Opportunities to Reduce Fragmentation,  
20 Overlap, and Duplication and Achieve  
21 Other Financial Benefits” (GAO-16-  
22 375SP), published on April 13, 2016;

23 (iii) Government Accountability Office  
24 Report “Information Technology: DoD  
25 Needs to Fully Implement Program for Pi-

1           loting Open Source Software” (GAO-19-  
2           457), published on September 10, 2019;

3           (iv) Government Accountability Office  
4           Report “Information Technology: Federal  
5           Agencies and OMB Need to Continue to  
6           Improve Management and Cybersecurity”  
7           (GAO-20-691T), published on August 3,  
8           2020; and

9           (v) Government Accountability Office  
10          Report “DoD Software Licenses: Better  
11          Guidance and Plans Needed to Ensure Re-  
12          strictive Practices are Mitigated” (GAO-  
13          23-106290), published on September 12,  
14          2023.

15          (C) TECHNOLOGICAL FRAGMENTATION.—

16          The isolated development efforts of each agency  
17          contribute to a landscape of fragmented tech-  
18          nologies that impede interoperability and data  
19          exchange between Federal systems.

20          (D) SLOW ADOPTION OF BEST PRAC-

21          TICES.—The lack of software sharing hinders  
22          the diffusion of engineering best practices and  
23          innovations across agencies, whereas learning  
24          from the successes and failures of other agen-

1           cies would accelerate the modernization of gov-  
2           ernment systems.

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

10          (F) PUBLIC ACCOUNTABILITY.—Software  
11          funded by taxpayers should be available for  
12          scrutiny by the public to the greatest extent  
13          possible, to ensure transparency and account-  
14          ability.

15          (G) PILOT SUCCESS.—Preliminary initia-  
16          tives aimed at making Federally-funded custom-  
17          developed code freely available to the public  
18          have demonstrated the viability and benefits of  
19          such sharing schemes, including—

20               (i) Memorandum M–16–21 issued by  
21               the Office of Management and Budget on  
22               August 8, 2016, entitled “Federal Source  
23               Code Policy: Achieving Efficiency, Trans-  
24               parency, and Innovation through Reusable  
25               and Open Source Software”; and

1 (ii) “Code.gov”, which documents how  
2 agencies already extensively use public re-  
3 positories, demonstrating the ability of  
4 agencies to share code using existing infra-  
5 structure.

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

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

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

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

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

4           (4) enhancing transparency by making Feder-  
5           ally-funded custom-developed code available for pub-  
6           lic scrutiny, subject to necessary security consider-  
7           ations; and

8           (5) leveraging inter-agency collaboration for  
9           better security auditing of the shared codebase, aim-  
10          ing for a more unified and secure technological in-  
11          frastructure across agencies.

12 **SEC. 3. DEFINITIONS.**

13         In this Act:

14           (1) AGENCY.—The term “agency” has the  
15           meaning given that term in section 3502 of title 44,  
16           United States Code.

17           (2) CUSTOM-DEVELOPED CODE.—The term  
18           “custom-developed code”—

19                 (A) means source code that is—

20                         (i) produced in the performance of a  
21                         Federal contract or is otherwise fully fund-  
22                         ed by the Federal Government; or

23                         (ii) developed by a Federal employee  
24                         as part of the official duties of the em-  
25                         ployee;

1 (B) includes—

2 (i) source code, or segregable portions  
3 of source code, for which the Federal Gov-  
4 ernment could obtain unlimited rights  
5 under part 27 of the Federal Acquisition  
6 Regulation or any relevant supplemental  
7 acquisition regulations of an agency; and

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

11 (C) does not include—

12 (i) source code that is solely explor-  
13 atory or disposable in nature, including  
14 source code written by a developer experi-  
15 menting with a new language or library; or

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

18 (3) FEDERAL CHIEF INFORMATION OFFICER.—

19 The term “Federal Chief Information Officer”  
20 means the Administrator of the Office of Electronic  
21 Government.

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

1           (5) METADATA.—The term “metadata”, with  
2           respect to custom-developed code—

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

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

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

10                           (ii) is shared in a public or private re-  
11                           pository, and includes a hyperlink to the  
12                           repository, as applicable.

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

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

17                   (B) access to which is restricted to author-  
18                   ized users.

19           (7) PUBLIC REPOSITORY.—The term “public  
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 open to the public.

24           (8) SOFTWARE.—The term “software” has the  
25           meaning given the term “computer software” in sec-



1       tion 2.101 of title 48, Code of Federal Regulations,  
2       or any successor regulation.

3           (9) SOURCE CODE.—The term “source code”  
4       means a collection of computer commands written in  
5       a computer programming language that a computer  
6       can execute as a piece of software.

7       **SEC. 4. SOFTWARE REUSE.**

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

11           (1) the custom-developed code of the agency is  
12      contained at not less than 1 public or private reposi-  
13      tory and is accessible to Federal employees via pro-  
14      cedures developed under subsection  
15      (d)(1)(A)(ii)(III); and

16           (2) all software and other key technical compo-  
17      nents, including documentation, data models,  
18      schemas, metadata, and architecture designs, are  
19      owned by the agency.

20      (b) SOFTWARE REUSE RIGHTS IN PROCUREMENT  
21      CONTRACTS.—

22           (1) IN GENERAL.—The head of an agency that  
23      enters into a contract for the custom development of  
24      software shall acquire and enforce rights sufficient  
25      to enable the Governmentwide access, execution, and

1 modification of the custom-developed code relating to  
2 the software.

3 (2) BEST PRACTICES.—

4 (A) CONTRACT ADMINISTRATION.—With  
5 respect to a contract described in paragraph  
6 (1), the head of an agency shall ensure appro-  
7 priate contract administration and use of best  
8 practices to secure the full scope of licenses and  
9 rights for the Federal Government of the cus-  
10 tom-developed code developed under the con-  
11 tract, to allow for access, execution, and modi-  
12 fication by other agencies.

13 (B) DEVELOPMENT PROCESS.—With re-  
14 spect to a contract described in paragraph (1),  
15 the head of an agency shall ensure the use of  
16 best practices to require and obtain the delivery  
17 of the custom-developed code, documentation of  
18 the custom-developed code, configuration and  
19 artifacts required to develop, build, test, and  
20 deploy the custom-developed code, and other as-  
21 sociated materials from the developer through-  
22 out the development process.

23 (c) DISCOVERY.—Not later than 210 days after the  
24 date of enactment of this Act, the head of each agency

1 shall make metadata for the custom-developed code of the  
2 agency publicly accessible.

3 (d) ACCOUNTABILITY MECHANISMS.—

4 (1) AGENCY CIOS.—Not later than 180 days  
5 after the date of enactment of this Act, the Chief In-  
6 formation Officer of each agency, in consultation  
7 with the Chief Acquisition Officer, or similar official,  
8 of the agency and the Federal Chief Information Of-  
9 ficer, shall develop an agency-wide policy that—

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

12 (i) ensuring that agency custom-devel-  
13 oped code follows best practices for oper-  
14 ating repositories and version control sys-  
15 tems to keep track of changes and to facili-  
16 tate collaboration among multiple devel-  
17 opers;

18 (ii) managing the sharing and dis-  
19 covery of source code, including devel-  
20 oping—

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

1 (II) procedures for making  
2 metadata for custom-developed code  
3 discoverable, pursuant to section 4(e);

4 (III) procedures for Federal em-  
5 ployees to discover and gain access to  
6 private repositories;

7 (IV) standardized reporting prac-  
8 tices across the agency to capture key  
9 information relating to a contract for  
10 reporting statistics about the contract;  
11 and

12 (V) procedures for updating  
13 metadata, private repositories, and  
14 public repositories on a quarterly  
15 basis;

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

19 (iv) if practicable, using existing pro-  
20 cedures and systems; and

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

24 (2) FEDERAL CIO.—

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

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

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

19 (ii) whether the shared code is main-  
20 tained;

21 (iii) whether there is a feedback mech-  
22 anism for improvements to or community  
23 development of the shared code; and

1 (iv) the number and circumstances of  
2 all exemptions granted under section  
3 5(b)(2).

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

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

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

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

19 **SEC. 5. SCOPE AND APPLICABILITY.**

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

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

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

4           (b) EXEMPTIONS.—

5           (1) AUTOMATIC.—This Act shall not apply to  
6           classified source code or source code developed pri-  
7           marily for use in a national security system, as de-  
8           fined in section 11103 of title 40, United States  
9           Code.

10          (2) EXPLANATION REQUIRED.—

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

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

22           (i) The sharing or discovery of the  
23           source code is restricted by Federal law or  
24           regulation, including the Export Adminis-  
25           tration Regulations, the International

1 Traffic in Arms Regulations, regulations of  
2 the Transportation Security Administra-  
3 tion relating to the protection of Sensitive  
4 Security Information, and the Federal laws  
5 and regulations governing classified infor-  
6 mation.

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

10 **SEC. 6. GUIDANCE.**

11 The Director of the Office of Management and Budg-  
12 et shall issue guidance, consistent with the purpose of this  
13 Act, that establishes best practices and uniform proce-  
14 dures across agencies under section 4(d).

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

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

21 (1) duplicative software procurement across and  
22 within agencies, including estimates of the fre-  
23 quency, severity, and dollar value of the duplicative  
24 software 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  
8 the Comptroller General of the United States.

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

13           (1) the implementation of this Act; and

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

16 **SEC. 8. RULE OF CONSTRUCTION.**

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

22 **SEC. 9. NO ADDITIONAL FUNDING.**

23           No additional funds are authorized to be appro-  
24 priated to carry out this Act.