

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

**IN THE SENATE OF THE UNITED STATES—118th Cong., 2d Sess.**

**S. 3594**

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

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended  
to be proposed by Mr. PETERS

Viz:

1 Strike all after the enacting clause and insert the fol-  
2 lowing:

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  
12 procurement of similar software solutions for

1 comparable problems, leading to a duplicative  
2 allocation of resources that could otherwise be  
3 avoided.

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

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

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

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

1           oting 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 federally  
5 funded custom-developed code available for public  
6 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) APPROPRIATE CONGRESSIONAL COMMIT-  
18 TEES.—The term “appropriate congressional com-  
19 mittees” means the Committee on Homeland Secu-  
20 rity and Governmental Affairs of the Senate and the  
21 Committee on Oversight and Accountability of the  
22 House of Representatives.

23           (3) 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 exclusively  
3 funded 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;

22 (ii) commercial computer software,  
23 commercial off-the-shelf software, or con-  
24 figuration scripts for such software; or

1 (iii) source code that is used in the  
2 performance of, but not produced in fulfill-  
3 ment of, a Federal contract.

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

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

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

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

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

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

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

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

24 (B) access to which is restricted to author-  
25 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 Administrator of the Office of  
16 Electronic Government, shall develop an agency-wide  
17 policy that—

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

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

1 (ii) managing the sharing and dis-  
2 covery 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(c);

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

14 (IV) procedures for checking the  
15 use of existing shared code as an al-  
16 ternative to initiating a new project or  
17 procurement;

18 (V) standardized reporting prac-  
19 tices across the agency to capture key  
20 information relating to a contract for  
21 reporting statistics about the contract;  
22 and

23 (VI) procedures for updating  
24 metadata, private repositories, and

1 public repositories on a quarterly  
2 basis;

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

6 (iv) if practicable, using existing pro-  
7 cedures and systems; and

8 (B) corrects or amends any policies of the  
9 agency that are inconsistent with the require-  
10 ments of this Act.

11 (2) ADMINISTRATOR OF THE OFFICE OF ELEC-  
12 TRONIC GOVERNMENT.—

13 (A) FRAMEWORK FOR REVIEW.—Not later  
14 than 1 year after the date of enactment of this  
15 Act, the Administrator of the Office of Elec-  
16 tronic Government shall establish a framework  
17 for reviewing the software being developed  
18 across the Federal Government to surface and  
19 support the goals of existing digital priorities,  
20 including issuing guidance on—

21 (i) the implementation of subsection  
22 (c);

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

1 (iii) other procedures for agencies to  
2 use to ensure that existing shared code has  
3 been considered as an alternative to initi-  
4 ating a new project or procurement;

5 (iv) identifying exemptions to this Act;  
6 and

7 (v) the frequency of and official re-  
8 sponsible for security auditing of reposi-  
9 tories.

10 (B) MINIMUM STANDARD REPORTING RE-  
11 QUIREMENTS.—Not later than 120 days after  
12 the date of enactment of this Act, the Adminis-  
13 trator of the Office of Electronic Government,  
14 in coordination with the Director of the Na-  
15 tional Institute of Standards and Technology,  
16 shall establish minimum standard reporting re-  
17 quirements for the Chief Information Officers  
18 of agencies, which shall include information re-  
19 lating to—

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

22 (ii) whether the shared code is main-  
23 tained;

- 1 (iii) whether there is a feedback mech-  
2 anism for improvements to or community  
3 development of the shared code; and  
4 (iv) the number and circumstances of  
5 all exemptions granted under section  
6 5(b)(2).

7 **SEC. 5. SCOPE AND APPLICABILITY.**

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

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

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

16 (b) EXEMPTIONS.—

17 (1) AUTOMATIC.—

18 (A) NATIONAL SECURITY.—An exemption  
19 from the requirements under section 4 shall  
20 apply to classified source code or source code  
21 developed—

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





1           sure consistent application of this para-  
2           graph across agencies.

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

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

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

19           (3) REPORTS REQUIRED.—

20                   (A) IN GENERAL.—Not later than Decem-  
21                  ber 31 of each year, the Chief Information Offi-  
22                  cer of an agency shall submit to the Adminis-  
23                  trator of the Office of Electronic Government a  
24                  report of the source code of the agency to which  
25                  an exemption under paragraph (1) or (2) ap-

1           plied during the fiscal year ending on Sep-  
2           tember 30 of that year with a brief narrative  
3           justification of each exemption.

4           (B) FORM.—The report under subpara-  
5           graph (A) shall be submitted in unclassified  
6           form, with a classified annex as appropriate.

7           (C) ANNUAL REPORT.—Not later than 1  
8           year after the date of enactment of this Act,  
9           and annually thereafter, the Administrator of  
10          the Office of Electronic Government shall sub-  
11          mit to the appropriate congressional committees  
12          a report on the status of the implementation of  
13          this Act by each agency, including—

14                 (i) a compilation of all information,  
15                 including a narrative justification, relating  
16                 to each exemption granted under para-  
17                 graphs (1) and (2);

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

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

25                 (iv) a classified annex as appropriate.

1 **SEC. 6. GUIDANCE.**

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

6 **SEC. 7. GAO REPORT ON INFORMATION TECHNOLOGY**  
7 **PRACTICES.**

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

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

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

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

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

25 (b) SUPPLEMENTAL REPORT.—Not later than 2  
26 years after the date of enactment of this Act, the Comp-

1 troller General of the United States shall submit to the  
2 appropriate congressional committees a report that in-  
3 cludes an assessment of—

4 (1) the implementation of this Act; and

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

7 **SEC. 8. RULE OF CONSTRUCTION.**

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

13 **SEC. 9. NO ADDITIONAL FUNDING.**

14 No additional funds are authorized to be appro-  
15 priated to carry out this Act.

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

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