

AMENDMENT TO RULES COMM. PRINT 119-33

OFFERED BY M .

Add at the end of subtitle A of title XVII the following:

1 **SEC. 17** . **REAUTHORIZATION OF CISA STATE AND LOCAL**
2 **CYBERSECURITY GRANT PROGRAM.**

3 Section 2220A of the Homeland Security Act of 2002
4 (6 U.S.C. 665g) is amended—

5 (1) in subsection (a)—

6 (A) by redesignating paragraphs (1), (2),
7 (3), (4), (5), (6), and (7) as paragraphs (3),
8 (4), (6), (9), (10), (11), and (12), respectively;

9 (B) by inserting before paragraph (3), as
10 so redesignated, the following new paragraphs:

11 “(1) **ARTIFICIAL INTELLIGENCE.**—The term
12 ‘artificial intelligence’ has the meaning given such
13 term in section 5002(3) of the National Artificial In-
14 telligence Initiative Act of 2020 (enacted as division
15 **E** of the William M. (Mac) Thornberry National De-
16 fense Authorization Act for Fiscal Year 2021 (15
17 U.S.C. 9401(3))).

18 “(2) **ARTIFICIAL INTELLIGENCE SYSTEM.**—The
19 term ‘artificial intelligence system’ means any data

1 system, software, hardware, application tool, or util-
2 ity that operates in whole or in part using artificial
3 intelligence.”;

4 (C) by inserting after paragraph (4), as so
5 redesignated, the following new paragraphs:

6 “(5) FOREIGN ENTITY OF CONCERN.—The
7 term ‘foreign entity of concern’ has the meaning
8 given such term in section 10634 of the Research
9 and Development, Competition, and Innovation Act
10 (42 U.S.C. 19237; Public Law 117–167; popularly
11 referred to as the ‘CHIPS and Science Act’).

12 “(6) MILITARY INSTALLATION.—The term
13 ‘military installation’ has the meaning given such
14 term in section 2801 of title 10, United States
15 Code.”; and

16 (D) by inserting after paragraph (7), as so
17 redesignated, the following new paragraph:

18 “(8) MULTI-FACTOR AUTHENTICATION.—The
19 term ‘multi factor authentication’ means an authen-
20 tication system that requires more than one distinct
21 type of authentication factor for successful authen-
22 tication of a user, including by using a multi-factor
23 authenticator or by combining single-factor authen-
24 ticators that provide different types of factors.”;

1 (2) in subsection (b)(1), by striking “informa-
2 tion systems owned” and inserting “information sys-
3 tems or operational technology systems, including ei-
4 ther or both of such systems using artificial intel-
5 ligence, maintained, owned,”;

6 (3) in subsection (d)(4), by striking “to the in-
7 formation systems owned” and inserting “to the in-
8 formation systems or operational technology sys-
9 tems, including either or both of such systems using
10 artificial intelligence, maintained, owned,”;

11 (4) in subsection (e)—

12 (A) in paragraph (2)—

13 (i) in subparagraph (A)(i), by striking
14 “information systems owned” and insert-
15 ing “information systems or operational
16 technology systems, including either or
17 both of such systems using artificial intel-
18 ligence, maintained, owned,”;

19 (ii) in subparagraph (B)—

20 (I) by amending clauses (i)
21 through (v) to read as follows:

22 “(i) manage, monitor, and track appli-
23 cations, user accounts, and information
24 systems and operational technology sys-
25 tems, including either or both of such sys-

1 tems using artificial intelligence, that are
2 maintained, owned, or operated by, or on
3 behalf of, the eligible entity, or, if the eligi-
4 ble entity is a State, local governments
5 within the jurisdiction of the eligible entity,
6 and the information technology deployed
7 on such information systems or operational
8 technology systems (as the case may be),
9 including legacy information systems, oper-
10 ational technology systems, and informa-
11 tion technology that are no longer sup-
12 ported by the manufacturer of the systems
13 or technology at issue;

14 “(ii) monitor, audit, and track net-
15 work traffic and activity transiting or trav-
16 eling to or from applications, user ac-
17 counts, and information systems and oper-
18 ational technology systems, including either
19 or both of such systems using artificial in-
20 telligence, maintained, owned, or operated
21 by, or on behalf of, the eligible entity or,
22 if the eligible entity is a State, local gov-
23 ernments within the jurisdiction of the eli-
24 gible entity;

1 “(iii) enhance the preparation, re-
2 sponse, and resiliency of applications, user
3 accounts, and information systems and
4 operational technology systems, including
5 either or both of such systems using artifi-
6 cial intelligence, maintained, owned, or op-
7 erated by, or on behalf of, the eligible enti-
8 ty or, if the eligible entity is a State, local
9 governments within the jurisdiction of the
10 eligible entity, against cybersecurity risks
11 and cybersecurity threats;

12 “(iv) implement a process of contin-
13 uous cybersecurity vulnerability assess-
14 ments and threat mitigation practices
15 prioritized by degree of risk to address cy-
16 bersecurity risks and cybersecurity threats
17 on applications, user accounts, and infor-
18 mation systems and operational technology
19 systems, including either or both of such
20 systems using artificial intelligence, main-
21 tained, owned, or operated by, or on behalf
22 of, the eligible entity or, if the eligible enti-
23 ty is a State, local governments within the
24 jurisdiction of the eligible entity;

1 “(v) ensure that the eligible entity
2 and, if the eligible entity is a State, local
3 governments within the jurisdiction of the
4 eligible entity, adopt and use best practices
5 and methodologies to enhance cybersecu-
6 rity, particularly identity and access man-
7 agement solutions such as multi-factor au-
8 thentication, which may include—

9 “(I) the practices set forth in a
10 cybersecurity framework developed by
11 the National Institute of Standards
12 and Technology or the Agency;

13 “(II) cyber chain supply chain
14 risk management best practices iden-
15 tified by the National Institute of
16 Standards and Technology or the
17 Agency;

18 “(III) knowledge bases of adver-
19 sary tools and tactics;

20 “(IV) technologies such as artifi-
21 cial intelligence; and

22 “(V) improving cyber incident re-
23 sponse capabilities through adoption
24 of automated cybersecurity prac-
25 tices;”;

1 (II) by amending clause (x) to
2 read as follows:

3 “(x) assess and mitigate, to the great-
4 est degree possible, cybersecurity risks and
5 cybersecurity threats relating to critical in-
6 frastructure and key resources, the deg-
7 radation of which may impact the perform-
8 ance of information systems or operational
9 technology systems, including either or
10 both of such systems using artificial intel-
11 ligence, within the jurisdiction of the eligi-
12 ble entity, including—

13 “(I) water and wastewater sys-
14 tems, electric power generation and
15 distribution systems, natural gas and
16 liquid fuel pipeline and distribution
17 systems, communications infrastruc-
18 ture (including broadband networks,
19 telecommunications systems, and
20 emergency communications networks),
21 transportation networks, and port and
22 maritime facilities, that directly serve
23 or support a military installation lo-
24 cated within or proximate to the juris-
25 diction of the eligible entity, the dis-

1 ruption of which by a cybersecurity
2 incident could degrade military readi-
3 ness, impede mobilization or
4 sustainment of military forces, or oth-
5 erwise affect national security; and

6 “(II) any other critical infra-
7 structure upon which the defense in-
8 dustrial base sector is operationally
9 dependent;”.

10 (III) in clause (xi)(I), by insert-
11 ing “, including through Department
12 of Homeland Security State, Local,
13 and Regional Fusion Center Initiative
14 under section 210(A)” before the
15 semicolon;

16 (IV) in clause (xii), by inserting
17 “, including for bolstering the resil-
18 ience of outdated or vulnerable infor-
19 mation systems or operational tech-
20 nology systems, including either or
21 both of such systems using artificial
22 intelligence” before the semicolon;

23 (V) by amending clause (xiii) to
24 read as follows:

1 “(xiii) implement an information tech-
2 nology or operational technology, including
3 either or both of such systems using artifi-
4 cial intelligence, modernization cybersecu-
5 rity review process that ensures alignment
6 between information technology, oper-
7 ational technology, and artificial intel-
8 ligence cybersecurity objectives;”;

9 (VI) in clause (xiv)(II)—

10 (aa) in item (aa), by striking

11 “and” after the semicolon;

12 (bb) in item (bb), by insert-
13 ing “and” after the semicolon;
14 and

15 (cc) by adding at the end
16 the following new item:

17 “(cc) academic and non-
18 profit entities, including cyberse-
19 curity clinics and other nonprofit
20 technical assistance programs;”;
21 and

22 (VII) by amending clause (xv) to
23 read as follows:

24 “(xv) ensure adequate access to, and
25 participation in, the services and programs

1 described in this subparagraph by rural
2 areas and other local governments with
3 small populations within the jurisdiction of
4 the eligible entity, including by direct out-
5 reach to such rural areas and local govern-
6 ments with small populations; and”;

7 (iii) in subparagraph (F)—

8 (I) in clause (i), by striking
9 “and” after the semicolon;

10 (II) by amending clause (ii) to
11 read as follows:

12 “(ii) reducing cybersecurity risks to,
13 and identifying, responding to, and recov-
14 ering from cybersecurity threats to, infor-
15 mation systems or operational technology
16 systems, including either or both of such
17 systems using artificial intelligence, main-
18 tained, owned or operated by, or on behalf
19 of, the eligible entity or, if the eligible enti-
20 ty is a State, local governments within the
21 jurisdiction of the eligible entity; and”;

22 (III) by adding at the end the
23 following new clause:

1 “(iii) assuming the cost or partial cost
2 of cybersecurity investments made as a re-
3 sult of the plan.”; and

4 (B) in paragraph (3)(A), by striking “the
5 Multi-State Information Sharing and Analysis
6 Center” and inserting “Information Sharing
7 and Analysis Organizations”;

8 (5) in subsection (g)—

9 (A) in paragraph (2)(A)(ii), by inserting
10 “including, as appropriate, representatives of
11 rural, suburban, and high-population jurisdic-
12 tions (including such jurisdictions with low or
13 otherwise limited operating budgets)” before
14 the semicolon; and

15 (B) by amending paragraph (5) to read as
16 follows:

17 “(5) RULE OF CONSTRUCTION REGARDING CON-
18 TROL OF CERTAIN INFORMATION SYSTEMS OR OPER-
19 ATIONAL TECHNOLOGY SYSTEMS OF ELIGIBLE ENTI-
20 TIES.—Nothing in this subsection may be construed
21 to permit a cybersecurity planning committee of an
22 eligible entity that meets the requirements of this
23 subsection to make decisions relating to information
24 systems or operational technology systems, including
25 either or both of such systems using artificial intel-

1 ligence, maintained, owned, or operated by, or on be-
2 half of, the eligible entity.”;

3 (6) in subsection (i)—

4 (A) in paragraph (1)(B), by striking “2-
5 year period” and inserting “3-year period”;

6 (B) in paragraph (3)—

7 (i) in the matter preceding subpara-
8 graph (A), by striking “2023” and insert-
9 ing “2027”; and

10 (ii) in subparagraph (B), by striking
11 “2023” and inserting “2027”; and

12 (C) in paragraph (4)—

13 (i) in the matter preceding subpara-
14 graph (A), by striking “shall” and insert-
15 ing “may”; and

16 (ii) in subparagraph (A), by striking
17 “information systems owned” and insert-
18 ing “information systems or operational
19 technology systems, including either or
20 both of such systems using artificial intel-
21 ligence, maintained, owned,”;

22 (7) in subsection (j)(1)—

23 (A) in subparagraph (D), by striking “or”
24 after the semicolon;

25 (B) in subparagraph (E)—

1 (i) by striking “information systems
2 owned” and inserting “information sys-
3 tems or operational technology systems, in-
4 cluding either or both of such systems
5 using artificial intelligence, maintained,
6 owned,”; and

7 (ii) by striking the period and insert-
8 ing a semicolon; and

9 (C) by adding at the end the following new
10 subparagraphs:

11 “(F) to purchase software or hardware, or
12 products or services of such software or hard-
13 ware, as the case may be, that do not align with
14 guidance relevant to such software or hardware,
15 or products or services, as the case may be, pro-
16 vided by the Agency, including Secure by De-
17 sign or successor guidance; or

18 “(G) to purchase software or hardware, or
19 products or services of such software or hard-
20 ware, as the case may be, that are designed, de-
21 veloped, operated, maintained, manufactured, or
22 sold by a foreign entity of concern and do not
23 align with guidance provided by the Agency.”;

1 (8) in subsection (l), in the matter preceding
2 paragraph (1), by striking “2022” and inserting
3 “2026”;

4 (9) in subsection (m), by amending paragraph
5 (1) to read as follows:

6 “(1) IN GENERAL.—The Federal share of ac-
7 tivities carried out using funds made available pur-
8 suant to the award of a grant under this section
9 may not exceed—

10 “(A) in the case of a grant to an eligible
11 entity, 60 percent for each fiscal year through
12 fiscal year 2033; and

13 “(B) in the case of a grant to a multi-enti-
14 ty group, 70 percent for each fiscal year
15 through fiscal year 2033.

16 Notwithstanding subparagraphs (A) and (B), the
17 Federal share of the cost for an eligible entity or
18 multi-entity group shall be 65 percent for an entity
19 and 75 percent for a multi-group entity for each fis-
20 cal year beginning with fiscal year 2028 through fis-
21 cal year 2033 if such entity or multi-entity group
22 entity, as the case may be, implements or enables,
23 by not later than October 1, 2027, multi-factor au-
24 thentication and identity and access management
25 tools that support multi-factor authentication with

1 respect to critical infrastructure, including the infor-
2 mation systems and operational technology systems,
3 including either or both of such systems using artifi-
4 cial intelligence, of such critical infrastructure, that
5 is within the jurisdiction of such entity or multi-enti-
6 ty group is responsible.”;

7 (10) in subsection (n)—

8 (A) in paragraph (2)—

9 (i) in subparagraph (A)—

10 (I) in the matter preceding clause

11 (i), by striking “a grant” and insert-

12 ing “a grant on or after January 1,

13 2026, or changes the allocation of

14 funding as permissible within the al-

15 lowances”; and

16 (II) by amending clauses (ii) and

17 (iii) to read as follows:

18 “(ii) with the consent of the local gov-

19 ernments, items, in-kind services, capabili-

20 ties, or activities, or a combination of fund-

21 ing and other services, having a value of

22 not less than 80 percent of the amount of

23 the grant; or

24 “(iii) with the consent of the local

25 governments, grant funds combined with

1 other items, in-kind services, capabilities,
2 or activities, or a combination of funding
3 and other services, having the total value
4 of not less than 80 percent of the amount
5 of the grant.”; and

6 (ii) in subparagraph (B), by amending
7 clauses (ii) and (iii) to read as follows:

8 “(ii) items, in kind services, capabili-
9 ties, or activities, or a combination of fund-
10 ing and other services, having a value of
11 not less than 25 percent of the amount of
12 the grant awarded to the eligible entity; or

13 “(iii) grant funds combined with other
14 items, in kind services, capabilities, or ac-
15 tivities, or a combination of funding and
16 other services, having the total value of not
17 less than 25 percent of the grant awarded
18 to the eligible entity.”; and

19 (B) by amending paragraph (5) to read as
20 follows:

21 “(5) DIRECT FUNDING.—If an eligible entity
22 does not make a distribution to a local government
23 required under paragraph (2) within 60 days of the
24 anticipated grant disbursement date, such local gov-
25 ernment may petition the Secretary to request the

1 Secretary to provide funds directly to such local gov-
2 ernment.”;

3 (11) in subsection (o), in the matter preceding
4 paragraph (1), by inserting “and representatives
5 from rural areas and other local governments with
6 small populations” after “governments”;

7 (12) by redesignating subsections (p) through
8 (s) as subsections (q) through (t), respectively;

9 (13) by inserting after subsection (o) the fol-
10 lowing new subsection:

11 “(p) OUTREACH TO LOCAL GOVERNMENTS.—The
12 Secretary, acting through the Director, shall implement an
13 outreach plan to inform local governments, including those
14 in rural areas or with small populations, about no-cost cy-
15 bersecurity service offerings available from the Agency.”;

16 (14) in subsection (r), as so redesignated—

17 (A) in paragraph (1)(A)—

18 (i) in clause (i), by striking “and”
19 after the semicolon;

20 (ii) in clause (ii)—

21 (I) by striking “information sys-
22 tems owned” and inserting “informa-
23 tion systems or operational technology
24 systems, including either or both of

1 such systems using artificial intel-
2 ligence, maintained, owned,”; and

3 (II) by striking the period and
4 inserting “; and”; and

5 (iii) by adding at the end the fol-
6 lowing new clause:

7 “(iii) assuming the costs associated
8 with continuing the programs specified in
9 the Cybersecurity Plan by including such
10 programs in State and local government
11 budgets upon full expenditure of grant
12 funds by the eligible entity.”;

13 (B) in paragraph (2)—

14 (i) in subparagraph (D), by striking
15 “and” after the semicolon;

16 (ii) in subparagraph (E)(ii)—

17 (I) by striking “information sys-
18 tems owned” and inserting “informa-
19 tion systems or operational technology
20 systems, including either or both of
21 such systems using artificial intel-
22 ligence, maintained, owned”; and

23 (II) by striking the period and
24 inserting “; and”; and

1 (iii) by adding at the end the fol-
2 lowing new subparagraph:

3 “(F) a description of steps taken by eligi-
4 ble entities to assess and mitigate, pursuant to
5 subsection (e)(2)(B)(x), cybersecurity risks and
6 cybersecurity threats to critical infrastructure
7 that serves or supports military installations
8 within or proximate to the jurisdictions of such
9 eligible entities, and an identification of any sig-
10 nificant challenges encountered by such eligible
11 entities in so assessing and mitigating such
12 risks and threats.”; and

13 (C) by amending paragraph (6) to read as
14 follows:

15 “(6) GAO REVIEW.—Not later than three years
16 after the date of the enactment of this paragraph
17 and every three years thereafter until the termi-
18 nation of the State and Local Cybersecurity Grant
19 Program, the Comptroller General of the United
20 States shall conduct a review of the Program, in-
21 cluding relating to the following:

22 “(A) The grant selection process of the
23 Secretary.

24 “(B) A sample of grants awarded under
25 this section.

1 “(C) A review of artificial intelligence
2 adoption across the sample of grants re-
3 viewed.”;

4 (15) in subsection (s), as so redesignated, by
5 amending paragraph (1) to read as follows:

6 “(1) IN GENERAL.—The activities under this
7 section are subject to the availability of appropria-
8 tions.”; and

9 (16) in subsection (t), as so redesignated, in
10 paragraph (1), by striking “2026” and inserting
11 “2033”.

