

AMENDMENT TO RULES COMM. PRINT 119–8
OFFERED BY MR. GARBARINO OF NEW YORK

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

1 SEC. 1703. 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), (8), (9), (10), and (11), 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 paragraph:

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’).”; and

12 (D) by inserting after paragraph (6), as so
13 redesignated, the following new paragraph:

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

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

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

6 (4) in subsection (e)—

7 (A) in paragraph (2)—

8 (i) in subparagraph (A)(i), by striking
9 “information systems owned” and insert-
10 ing “information systems or operational
11 technology systems, including either or
12 both of such systems using artificial intel-
13 ligence, maintained, owned, or”;

14 (ii) in subparagraph (B)—

15 (I) by amending clauses (i)
16 through (v) to read as follows:

17 “(i) manage, monitor, and track appli-
18 cations, user accounts, and information
19 systems and operational technology sys-
20 tems, including either or both of such sys-
21 tems using artificial intelligence, that are
22 maintained, owned, or operated by, or on
23 behalf of, the eligible entity, or, if the eligi-
24 ble entity is a State, local governments
25 within the jurisdiction of the eligible entity,

1 and the information technology deployed
2 on such information systems or operational
3 technology systems (as the case may be),
4 including legacy information systems, oper-
5 ational technology systems, and informa-
6 tion technology that are no longer sup-
7 ported by the manufacturer of the systems
8 or technology at issue;

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

20 “(iii) enhance the preparation, re-
21 sponse, and resiliency of applications, user
22 accounts, and information systems and
23 operational technology systems, including
24 either or both of such systems using artifi-
25 cial intelligence, maintained, owned, or op-

1 erated by, or on behalf of, the eligible enti-
2 ty or, if the eligible entity is a State, local
3 governments within the jurisdiction of the
4 eligible entity, against cybersecurity risks
5 and cybersecurity threats;

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

19 “(v) ensure that the eligible entity
20 and, if the eligible entity is a State, local
21 governments within the jurisdiction of the
22 eligible entity, adopt and use best practices
23 and methodologies to enhance cybersecu-
24 rity, particularly identity and access man-

1 agement solutions such as multi-factor au-
2 thentication, which may include—

3 “(I) the practices set forth in a
4 cybersecurity framework developed by
5 the National Institute of Standards
6 and Technology or the Agency;

7 “(II) cyber chain supply chain
8 risk management best practices iden-
9 tified by the National Institute of
10 Standards and Technology or the
11 Agency;

12 “(III) knowledge bases of adver-
13 sary tools and tactics;

14 “(IV) technologies such as artifi-
15 cial intelligence; and

16 “(V) improving cyber incident re-
17 sponse capabilities through adoption
18 of automated cybersecurity prac-
19 tices;”;

20 (II) in clause (x), by inserting
21 “or operational technology systems,
22 including either or both of such sys-
23 tems using artificial intelligence,”
24 after “information systems”;

1 (III) in clause (xi)(I), by insert-
2 ing “, including through Department
3 of Homeland Security State, Local,
4 and Regional Fusion Center Initiative
5 under section 210(A)” before the
6 semicolon; and

7 (IV) in clause (xii), by inserting
8 “, including for bolstering the resil-
9 ience of outdated or vulnerable infor-
10 mation systems or operational tech-
11 nology systems, including either or
12 both of such systems using artificial
13 intelligence” before the semicolon;

14 (V) by amending clause (xiii) to
15 read as follows:

16 “(xiii) implement an information tech-
17 nology or operational technology, including
18 either or both of such systems using artifi-
19 cial intelligence, modernization cybersecu-
20 rity review process that ensures alignment
21 between information technology, oper-
22 ational technology, and artificial intel-
23 ligence cybersecurity objectives;”;

24 (VI) in clause (xiv)(II)—

1 (aa) in item (aa), by striking
2 “and” after the semicolon;
3 (bb) in item (bb), by insert-
4 ing “and” after the semicolon;
5 and
6 (cc) by adding at the end
7 the following new item:
8 “(cc) academic and non-
9 profit entities, including cyberse-
10 curity clinics and other nonprofit
11 technical assistance programs;”;
12 and
13 (VII) by amending clause (xv) to
14 read as follows:
15 “(xv) ensure adequate access to, and
16 participation in, the services and programs
17 described in this subparagraph by rural
18 areas and other local governments with
19 small populations within the jurisdiction of
20 the eligible entity, including by direct out-
21 reach to such rural areas and local govern-
22 ments with small populations; and”; and
23 (iii) in subparagraph (F)—
24 (I) in clause (i), by striking
25 “and” after the semicolon;

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

3 “(ii) reducing cybersecurity risks to,
4 and identifying, responding to, and recov-
5 ering from cybersecurity threats to, infor-
6 mation systems or operational technology
7 systems, including either or both of such
8 systems using artificial intelligence, main-
9 tained, owned or operated by, or on behalf
10 of, the eligible entity or, if the eligible enti-
11 ty is a State, local governments within the
12 jurisdiction of the eligible entity; and”;

13 (III) by adding at the end the
14 following new clause:

15 “(iii) assuming the cost or partial cost
16 of cybersecurity investments made as a re-
17 sult of the plan.”; and

18 (B) in paragraph (3)(A), by striking “the
19 Multi-State Information Sharing and Analysis
20 Center” and inserting “Information Sharing
21 and Analysis Organizations”;

22 (5) in subsection (g)—

23 (A) in paragraph (2)(A)(ii), by inserting
24 “including, as appropriate, representatives of
25 rural, suburban, and high-population jurisdic-

1 tions (including such jurisdictions with low or
2 otherwise limited operating budgets)” before
3 the semicolon; and

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

6 “(5) RULE OF CONSTRUCTION REGARDING CON-
7 TROL OF CERTAIN INFORMATION SYSTEMS OR OPER-
8 ATIONAL TECHNOLOGY SYSTEMS OF ELIGIBLE ENTI-
9 TIES.—Nothing in this subsection may be construed
10 to permit a cybersecurity planning committee of an
11 eligible entity that meets the requirements of this
12 subsection to make decisions relating to information
13 systems or operational technology systems, including
14 either or both of such systems using artificial intel-
15 ligence, maintained, owned, or operated by, or on be-
16 half of, the eligible entity.”;

17 (6) in subsection (i)—

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

20 (B) in paragraph (3)—

21 (i) in the matter preceding subpara-
22 graph (A), by striking “2023” and insert-
23 ing “2027”; and

24 (ii) in subparagraph (B), by striking
25 “2023” and inserting “2027”; and

1 (C) in paragraph (4)—

2 (i) in the matter preceding subpara-
3 graph (A), by striking “shall” and insert-
4 ing “may”; and

5 (ii) in subparagraph (A), by striking
6 “information systems owned” inserting
7 “information systems or operational tech-
8 nology systems, including either or both of
9 such systems using artificial intelligence,
10 maintained, owned,”;

11 (7) in subsection (j)(1)—

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

14 (B) in subparagraph (E)—

15 (i) by striking “information systems
16 owned” and inserting “information sys-
17 tems or operational technology systems, in-
18 cluding either or both of such systems
19 using artificial intelligence, maintained,
20 owned,”; and

21 (ii) by striking the period and insert-
22 ing a semicolon; and

23 (C) by adding at the end the following new
24 subparagraphs:

1 “(E) to purchase software or hardware, or
2 products or services of such software or hard-
3 ware, as the case may be, that do not align with
4 guidance relevant to such software or hardware,
5 or products or services, as the case may be, pro-
6 vided by the Agency, including Secure by De-
7 sign or successor guidance; or

8 “(F) to purchase software or hardware, or
9 products or services of such software or hard-
10 ware, as the case may be, that are designed, de-
11 veloped, operated, maintained, manufactured, or
12 sold by a foreign entity of concern and do not
13 align with guidance provided by the Agency.”;

14 (8) in subsection (l), in the matter preceding
15 paragraph (1), by striking “2022” and inserting
16 “2026”;

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

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

23 “(A) in the case of a grant to an eligible
24 entity, 60 percent for each fiscal year through
25 fiscal year 2035; and

1 “(B) in the case of a grant to a multi-enti-
2 ty group, 70 percent for each fiscal year
3 through fiscal year 2035.

4 Notwithstanding subparagraphs (A) and (B), the
5 Federal share of the cost for an eligible entity or
6 multi-entity group shall be 65 percent for an entity
7 and 75 percent for a multi-group entity for each fis-
8 cal year beginning with fiscal year 2028 through fis-
9 cal year 2035 if such entity or multi-entity group
10 entity, as the case may be, implements or enables,
11 by not later than October 1, 2027, multi-factor au-
12 thentication and identity and access management
13 tools that support multi-factor authentication with
14 respect to critical infrastructure, including the infor-
15 mation systems and operational technology systems,
16 including either or both of such systems using artifi-
17 cial intelligence, of such critical infrastructure, that
18 is within the jurisdiction of such entity or multi-enti-
19 ty group is responsible.”;

20 (10) in subsection (n)—

21 (A) in paragraph (2)—

22 (i) in subparagraph (A)—

23 (I) in the matter preceding clause

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

25 ing “a grant on or after January 1,

1 2026, or changes the allocation of
2 funding as permissible within the al-
3 lowances of”; and

4 (II) by amending clauses (ii) and
5 (iii) to read as follows:

6 “(ii) with the consent of the local gov-
7 ernments, items, in-kind services, capabili-
8 ties, or activities, or a combination of fund-
9 ing and other services, having a value of
10 not less than 80 percent of the amount of
11 the grant; or

12 “(iii) with the consent of the local
13 governments, grant funds combined with
14 other items, in-kind services, capabilities,
15 or activities, or a combination of funding
16 and other services, having the total value
17 of not less than 80 percent of the amount
18 of the grant.”; and

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

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

1 “(iii) grant funds combined with other
2 items, in kind services, capabilities, or ac-
3 tivities, or a combination of funding and
4 other services, having the total value of not
5 less than 25 percent of the grant awarded
6 to the eligible entity.”; and

7 (B) by amending paragraph (5) to read as
8 follows:

9 “(5) DIRECT FUNDING.—If an eligible entity
10 does not make a distribution to a local government
11 required under paragraph (2) within 60 days of the
12 anticipated grant disbursement date, such local gov-
13 ernment may petition the Secretary to request the
14 Secretary to provide funds directly to such local gov-
15 ernment.”;

16 (11) in subsection (o), in the matter preceding
17 paragraph (1), by inserting “and representatives
18 from rural areas and other local governments with
19 small populations” after “governments”;

20 (12) by redesignating subsections (p) through
21 (s) as subsections (q) through (t), respectively;

22 (13) by inserting after subsection (o) the fol-
23 lowing new subsection:

24 “(p) OUTREACH TO LOCAL GOVERNMENTS.—The
25 Secretary, acting through the Director, shall implement an

1 outreach plan to inform local governments, including those
2 in rural areas or with small populations, about no-cost cy-
3 bersecurity service offerings available from the Agency.”;

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

5 (A) in paragraph (1)(A)—

6 (i) in clause (i), by striking “and”
7 after the semicolon;

8 (ii) in clause (ii)—

9 (I) by striking “information sys-
10 tems owned” inserting “information
11 systems or operational technology sys-
12 tems, including either or both of such
13 systems using artificial intelligence,
14 maintained, owned,”; and

15 (II) by striking the period and
16 inserting “; and”; and

17 (iii) by adding at the end the fol-
18 lowing new clause:

19 “(iii) assuming the costs associated
20 with continuing the programs specified in
21 the Cybersecurity Plan by including such
22 programs in State and local government
23 budgets upon full expenditure of grant
24 funds by the eligible entity.”;

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

7 (C) by amending paragraph (6) to read as
8 follows:

9 “(6) GAO REVIEW.—Not later than four years
10 after the date of the enactment of this paragraph
11 and every four years thereafter until the termination
12 of the State and Local Cybersecurity Grant Pro-
13 gram, the Comptroller General of the United States
14 shall conduct a review of the Program, including re-
15 lating to the following:

16 “(A) The grant selection process of the
17 Secretary.

18 “(B) A sample of grants awarded under
19 this section.

20 “(C) A review of artificial intelligence
21 adoption across the sample of grants re-
22 viewed.”;

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

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

4 (16) in subsection (t), as so redesignated, in
5 paragraph (1), by striking “2025” and inserting
6 “2035”.

