(C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

(b) Requirements

In carrying out CETAP, the Director shall—

(1) ensure that the program—

(A) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;

(B) conducts professional development sessions for teachers;

(C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);

(D) provides direct student engagement opportunities through camps and other programming;

(E) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;

(F) integrates with existing post-secondary education and workforce development programs at the Department;

(G) promotes and supports national standards for elementary and secondary cyber education;

(H) partners with cybersecurity and education stakeholder groups to expand outreach; and

(I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and

(2) enable the deployment of CETAP nationwide, with special consideration for underserved populations or communities.

(c) Briefings

(1) In general

Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

(2) Contents

Each briefing conducted under paragraph (1) shall include—

(A) estimated figures on the number of students reached and teachers engaged;

(B) information on outreach and engagement efforts, including the activities described in subsection (b)(1)(E);

(C) information on any grants or cooperative agreements made pursuant to subsection (e), including how any such grants or cooperative agreements are being used to enhance cybersecurity education for underserved populations or communities;

(D) information on new curricula offerings and teacher training platforms; and

(E) information on coordination with post-secondary education and workforce development programs at the Department.

(d) Mission promotion

The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel.

(e) Grants and cooperative agreements

The Director may award financial assistance in the form of grants or cooperative agreements to States, local governments, institutions of higher education (as such term is defined in section 1001 of title 20), nonprofit organizations, and other non-Federal entities as determined appropriate by the Director for the purpose of funding cybersecurity and infrastructure security education and training programs and initiatives to—

(1) carry out the purposes of CETAP; and

(2) enhance CETAP to address the national shortfall of cybersecurity professionals.

(Pub. L. 107–296, title XXII, § 2220, formerly § 2217, as added Pub. L. 116–283, div. A, title XVII, § 1719(c), Jan. 1, 2021, 134 Stat. 4106; renumbered § 2220 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(vii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7104, Dec. 23, 2022, 136 Stat. 3622.)

Editorial Notes

AMENDMENTS

2022—Subsec. (c)(2)(C) to (E). Pub. L. 117–263, § 7104(b), added subpar. (C) and redesignated former subpars. (C) and (D) as (D) and (E), respectively.

Subsec. (e). Pub. L. 117–263, § 7104(a), added subsec. (e).

2021—Pub. L. 117–81 reenacted section catchline.

§ 665g. State and Local Cybersecurity Grant Program

(a) Definitions

In this section:

(1) Cybersecurity Plan

The term ''Cybersecurity Plan'' means a plan submitted by an eligible entity under subsection (e)(1).

(2) Eligible entity

The term ''eligible entity'' means a—

(A) State; or

(B) Tribal government.

(3) Multi-entity group

The term ''multi-entity group'' means a group of 2 or more eligible entities desiring a grant under this section.

(4) Online service

The term ''online service'' means any internet-facing service, including a website, email, virtual private network, or custom application.

(5) Rural area

The term ''rural area'' has the meaning given the term in section 5302 of title 49.

(6) State and Local Cybersecurity Grant Program

The term ''State and Local Cybersecurity Grant Program'' means the program established under subsection (b).

(7) Tribal government

The term ''Tribal government'' means the recognized governing body of any Indian or

Alaska Native Tribe, band, nation, pueblo, village, community, component band, or component reservation, that is individually identified (including parenthetically) in the most recent list published pursuant to section 5131 of title 25.

(b) Establishment

(1) In general

There is established within the Department a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments.

(2) Application

An eligible entity desiring a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(c) Administration

The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 604 and 605 of this title.

(d) Use of funds

An eligible entity that receives a grant under this section and a local government that receives funds from a grant under this section, as appropriate, shall use the grant to—

(1) implement the Cybersecurity Plan of the eligible entity;

(2) develop or revise the Cybersecurity Plan of the eligible entity;

(3) pay expenses directly relating to the administration of the grant, which shall not exceed 5 percent of the amount of the grant;

(4) assist with activities that address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director, to the information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity; or

(5) fund any other appropriate activity determined by the Secretary, acting through the Director.

(e) Cybersecurity plans

(1) In general

An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for review in accordance with subsection (i).

(2) Required elements

A Cybersecurity Plan of an eligible entity shall—

(A) incorporate, to the extent practicable—

(i) any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, State, local, or Tribal governments; and

(ii) if the eligible entity is a State, consultation and feedback from local governments and associations of local governments within the jurisdiction of the eligible entity;

(B) describe, to the extent practicable, how the eligible entity will—

(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

(ii) monitor, audit, and,[1] track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(iii) enhance the preparation, response, and resiliency of information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, against cybersecurity risks and cybersecurity threats;

(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

(v) ensure that the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, adopt and use best practices and methodologies to enhance cybersecurity, such as—

(I) the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology;

(II) cyber chain supply chain risk management best practices identified by the National Institute of Standards and Technology; and

(III) knowledge bases of adversary tools and tactics;

(vi) promote the delivery of safe, recognizable, and trustworthy online services by the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including through the use of the .gov internet domain;

(vii) ensure continuity of operations of the eligible entity and, if the eligible enti-

[1] So in original. The comma probably should not appear.

ty is a State, local governments within the jurisdiction of the eligible entity, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident;

(viii) use the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

(ix) if the eligible entity is a State, ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local governments within the jurisdiction of the eligible entity in the event of an incident involving those communications or data networks;

(x) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity;

(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and—

(I) if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, including by expanding information sharing agreements with the Department; and

(II) the Department;

(xii) leverage cybersecurity services offered by the Department;

(xiii) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats in consultation with—

(I) if the eligible entity is a State, local governments and associations of local governments within the jurisdiction of the eligible entity; and

(II) as applicable—

(aa) eligible entities that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an Information Sharing and Analysis Organization; and

(bb) countries that neighbor the jurisdiction of the eligible entity;

(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the jurisdiction of the eligible entity; and

(xvi) distribute funds, items, services, capabilities, or activities to local governments under subsection (n)(2)(A), including the fraction of that distribution the eligible entity plans to distribute to rural areas under subsection (n)(2)(B);

(C) assess the capabilities of the eligible entity relating to the actions described in subparagraph (B);

(D) describe, as appropriate and to the extent practicable, the individual responsibilities of the eligible entity and local governments within the jurisdiction of the eligible entity in implementing the plan;

(E) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

(F) describe the metrics the eligible entity will use to measure progress towards—

(i) implementing the plan; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(3) Discretionary elements

In drafting a Cybersecurity Plan, an eligible entity may—

(A) consult with the Multi-State Information Sharing and Analysis Center;

(B) include a description of cooperative programs developed by groups of local governments within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

(C) include a description of programs provided by the eligible entity to support local governments and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

(f) Multi-entity grants

(1) In general

The Secretary may award grants under this section to a multi-entity group to support multi-entity efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities that comprise the multi-entity group.

(2) Satisfaction of other requirements

In order to be eligible for a multi-entity grant under this subsection, each eligible entity that comprises a multi-entity group shall have—

(A) a Cybersecurity Plan that has been reviewed by the Secretary in accordance with subsection (i); and

(B) a cybersecurity planning committee established in accordance with subsection (g).

(3) Application

(A) In general

A multi-entity group applying for a multi-entity grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(B) Multi-entity project plan

An application for a grant under this section of a multi-entity group under subparagraph (A) shall include a plan describing—

(i) the division of responsibilities among the eligible entities that comprise the multi-entity group;

(ii) the distribution of funding from the grant among the eligible entities that comprise the multi-entity group; and

(iii) how the eligible entities that comprise the multi-entity group will work together to implement the Cybersecurity Plan of each of those eligible entities.

(g) Planning committees

(1) In general

An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

(A) assist with the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

(B) approve the Cybersecurity Plan of the eligible entity; and

(C) assist with the determination of effective funding priorities for a grant under this section in accordance with subsections (d) and (j).

(2) Composition

A committee of an eligible entity established under paragraph (1) shall—

(A) be comprised of representatives from—

(i) the eligible entity;

(ii) if the eligible entity is a State, counties, cities, and towns within the jurisdiction of the eligible entity; and

(iii) institutions of public education and health within the jurisdiction of the eligible entity; and

(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(3) Cybersecurity expertise

Not less than one-half of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

(4) Rule of construction regarding existing planning committees

Nothing in this subsection shall be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that—

(A) meets the requirements of this subsection; or

(B) may be expanded or leveraged to meet the requirements of this subsection, including through the formation of a cybersecurity planning subcommittee.

(5) Rule of construction regarding control of information systems of eligible entities

Nothing in this subsection shall be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this subsection to make decisions relating to information systems owned or operated by, or on behalf of, the eligible entity.

(h) Special rule for Tribal governments

With respect to any requirement under subsection (e) or (g), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may prescribe an alternative substantively similar requirement for Tribal governments if the Secretary finds that the alternative requirement is necessary for the effective delivery and administration of grants to Tribal governments under this section.

(i) Review of plans

(1) Review as condition of grant

(A) In general

Subject to paragraph (3), before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall—

(i) review the Cybersecurity Plan of the eligible entity, including any revised Cybersecurity Plans of the eligible entity; and

(ii) determine that the Cybersecurity Plan reviewed under clause (i) satisfies the requirements under paragraph (2).

(B) Duration of determination

In the case of a determination under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), the determination shall be effective for the 2-year period beginning on the date of the determination.

(C) Annual renewal

Not later than 2 years after the date on which the Secretary determines under subparagraph (A)(ii) that a Cybersecurity Plan satisfies the requirements under paragraph (2), and annually thereafter, the Secretary, acting through the Director, shall—

(i) determine whether the Cybersecurity Plan and any revisions continue to meet the criteria described in paragraph (2); and

(ii) renew the determination if the Secretary, acting through the Director, makes a positive determination under clause (i).

(2) Plan requirements

In reviewing a Cybersecurity Plan of an eligible entity under this subsection, the Secretary, acting through the Director, shall ensure that the Cybersecurity Plan—

(A) satisfies the requirements of subsection (e)(2); and

(B) has been approved by—

(i) the cybersecurity planning committee of the eligible entity established under subsection (g); and

(ii) the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity.

(3) Exception

Notwithstanding subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary for review before September 30, 2023, if the eligible entity certifies to the Secretary that—

(A) the activities that will be supported by the grant are—

(i) integral to the development of the Cybersecurity Plan of the eligible entity; or

(ii) necessary to assist with activities described in subsection (d)(4), as confirmed by the Director; and

(B) the eligible entity will submit to the Secretary a Cybersecurity Plan for review under this subsection by September 30, 2023.

(4) Rule of construction

Nothing in this subsection shall be construed to provide authority to the Secretary to—

(A) regulate the manner by which an eligible entity or local government improves the cybersecurity of the information systems owned or operated by, or on behalf of, the eligible entity or local government; or

(B) condition the receipt of grants under this section on—

(i) participation in a particular Federal program; or

(ii) the use of a specific product or technology.

(j) Limitations on uses of funds

(1) In general

Any entity that receives funds from a grant under this section may not use the grant—

(A) to supplant State or local funds;

(B) for any recipient cost-sharing contribution;

(C) to pay a ransom;

(D) for recreational or social purposes; or

(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

(2) Compliance oversight

In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant under this section uses the grant for the purposes for which the grant is awarded.

(3) Rule of construction

Nothing in paragraph (1)(A) shall be construed to prohibit the use of funds from a grant under this section awarded to a State, local, or Tribal government for otherwise permissible uses under this section on the basis that the State, local, or Tribal government has previously used State, local, or Tribal funds to support the same or similar uses.

(k) Opportunity to amend applications

In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct any defects in those applications before making final awards, including by allowing applicants to revise a submitted Cybersecurity Plan.

***(l)* Apportionment**

For fiscal year 2022 and each fiscal year thereafter, the Secretary shall apportion amounts appropriated to carry out this section among eligible entities as follows:

(1) Baseline amount

The Secretary shall first apportion—

(A) 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the United States Virgin Islands;

(B) 1 percent of such amounts to each of the remaining States; and

(C) 3 percent of such amounts to Tribal governments.

(2) Remainder

The Secretary shall apportion the remainder of such amounts to States as follows:

(A) 50 percent of such remainder in the ratio that the population of each State, bears to the population of all States; and

(B) 50 percent of such remainder in the ratio that the population of each State that resides in rural areas, bears to the population of all States that resides in rural areas.

(3) Apportionment among Tribal governments

In determining how to apportion amounts to Tribal governments under paragraph (1)(C), the Secretary shall consult with the Secretary of the Interior and Tribal governments.

(4) Multi-entity grants

An amount received from a multi-entity grant awarded under subsection (f)(1) by a State or Tribal government that is a member of the multi-entity group shall qualify as an apportionment for the purpose of this subsection.

(m) Federal share

(1) In general

The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

(A) in the case of a grant to an eligible entity—

(i) for fiscal year 2022, 90 percent;

(ii) for fiscal year 2023, 80 percent;

(iii) for fiscal year 2024, 70 percent; and

(iv) for fiscal year 2025, 60 percent; and

(B) in the case of a grant to a multi-entity group—

(i) for fiscal year 2022, 100 percent;

(ii) for fiscal year 2023, 90 percent;

(iii) for fiscal year 2024, 80 percent; and

(iv) for fiscal year 2025, 70 percent.

(2) Waiver

(A) In general

The Secretary may waive or modify the requirements of paragraph (1) if an eligible en-

tity or multi-entity group demonstrates economic hardship.

(B) Guidelines

The Secretary shall establish and publish guidelines for determining what constitutes economic hardship for the purposes of this subsection.

(C) Considerations

In developing guidelines under subparagraph (B), the Secretary shall consider, with respect to the jurisdiction of an eligible entity—

(i) changes in rates of unemployment in the jurisdiction from previous years;

(ii) changes in the percentage of individuals who are eligible to receive benefits under the supplemental nutrition assistance program established under the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.) from previous years; and

(iii) any other factors the Secretary considers appropriate.

(3) Waiver for Tribal governments

Notwithstanding paragraph (2), the Secretary, in consultation with the Secretary of the Interior and Tribal governments, may waive or modify the requirements of paragraph (1) for 1 or more Tribal governments if the Secretary determines that the waiver is in the public interest.

(n) Responsibilities of grantees

(1) Certification

Each eligible entity or multi-entity group that receives a grant under this section shall certify to the Secretary that the grant will be used—

(A) for the purpose for which the grant is awarded; and

(B) in compliance with subsections (d) and (j).

(2) Availability of funds to local governments and rural areas

(A) In general

Subject to subparagraph (C), not later than 45 days after the date on which an eligible entity or multi-entity group receives a grant under this section, the eligible entity or multi-entity group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local governments within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multi-entity group—

(i) not less than 80 percent of funds available under the grant;

(ii) with the consent of the local governments, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

(iii) with the consent of the local governments, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

(B) Availability to rural areas

In obligating funds, items, services, capabilities, or activities to local governments under subparagraph (A), the eligible entity or eligible entities that comprise the multi-entity group shall ensure that rural areas within the jurisdiction of the eligible entity or the eligible entities that comprise the multi-entity group receive not less than—

(i) 25 percent of the amount of the grant awarded to the eligible entity;

(ii) items, services, capabilities, or activities having a value of not less than 25 percent of the amount of the grant awarded to the eligible entity; or

(iii) grant funds combined with other items, services, capabilities, or activities having the total value of not less than 25 percent of the grant awarded to the eligible entity.

(C) Exceptions

This paragraph shall not apply to—

(i) any grant awarded under this section that solely supports activities that are integral to the development or revision of the Cybersecurity Plan of the eligible entity; or

(ii) the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or a Tribal government.

(3) Certifications regarding distribution of grant funds to local governments

An eligible entity or multi-entity group shall certify to the Secretary that the eligible entity or multi-entity group has made the distribution to local governments required under paragraph (2).

(4) Extension of period

(A) In general

An eligible entity or multi-entity group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

(B) Approval

The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity Grant Program.

(5) Direct funding

If an eligible entity does not make a distribution to a local government required under paragraph (2) in a timely fashion, the local government may petition the Secretary to request the Secretary to provide funds directly to the local government.

(6) Limitation on construction

A grant awarded under this section may not be used to acquire land or to construct, re-

model, or perform alterations of buildings or other physical facilities.

(7) Consultation in allocating funds

An eligible entity applying for a grant under this section shall agree to consult the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity in allocating funds from a grant awarded under this section.

(8) Penalties

In addition to other remedies available to the Secretary, if an eligible entity violates a requirement of this subsection, the Secretary may—

(A) terminate or reduce the amount of a grant awarded under this section to the eligible entity; or

(B) distribute grant funds previously awarded to the eligible entity—

(i) in the case of an eligible entity that is a State, directly to the appropriate local government as a replacement grant in an amount determined by the Secretary; or

(ii) in the case of an eligible entity that is a Tribal government, to another Tribal government or Tribal governments as a replacement grant in an amount determined by the Secretary.

(*o*) Consultation with State, local, and Tribal representatives

In carrying out this section, the Secretary shall consult with State, local, and Tribal representatives with professional experience relating to cybersecurity, including representatives of associations representing State, local, and Tribal governments, to inform—

(1) guidance for applicants for grants under this section, including guidance for Cybersecurity Plans;

(2) the study of risk-based formulas required under subsection (q)(4);

(3) the development of guidelines required under subsection (m)(2)(B); and

(4) any modifications described in subsection (q)(2)(D).

(p) Notification to Congress

Not later than 3 business days before the date on which the Department announces the award of a grant to an eligible entity under this section, including an announcement to the eligible entity, the Secretary shall provide to the appropriate congressional committees notice of the announcement.

(q) Reports, study, and review

(1) Annual reports by grant recipients

(A) In general

Not later than 1 year after the date on which an eligible entity receives a grant under this section for the purpose of implementing the Cybersecurity Plan of the eligible entity, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in—

(i) implementing the Cybersecurity Plan of the eligible entity; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

(B) Absence of plan

Not later than 1 year after the date on which an eligible entity that does not have a Cybersecurity Plan receives funds under this section, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to—

(i) develop or revise a Cybersecurity Plan; or

(ii) assist with the activities described in subsection (d)(4).

(2) Annual reports to Congress

Not less frequently than annually, the Secretary, acting through the Director, shall submit to Congress a report on—

(A) the use of grants awarded under this section;

(B) the proportion of grants used to support cybersecurity in rural areas;

(C) the effectiveness of the State and Local Cybersecurity Grant Program;

(D) any necessary modifications to the State and Local Cybersecurity Grant Program; and

(E) any progress made toward—

(i) developing, implementing, or revising Cybersecurity Plans; and

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, State, local, or Tribal governments as a result of the award of grants under this section.

(3) Public availability

(A) In general

The Secretary, acting through the Director, shall make each report submitted under paragraph (2) publicly available, including by making each report available on the website of the Agency.

(B) Redactions

In making each report publicly available under subparagraph (A), the Director may make redactions that the Director, in consultation with each eligible entity, determines necessary to protect classified or other information exempt from disclosure under section 552 of title 5 (commonly referred to as the ''Freedom of Information Act'').

(4) Study of risk-based formulas

(A) In general

Not later than September 30, 2024, the Secretary, acting through the Director, shall

submit to the appropriate congressional committees a study and legislative recommendations on the potential use of a risk-based formula for apportioning funds under this section, including—

(i) potential components that could be included in a risk-based formula, including the potential impact of those components on support for rural areas under this section;

(ii) potential sources of data and information necessary for the implementation of a risk-based formula;

(iii) any obstacles to implementing a risk-based formula, including obstacles that require a legislative solution;

(iv) if a risk-based formula were to be implemented for fiscal year 2026, a recommended risk-based formula for the State and Local Cybersecurity Grant Program; and

(v) any other information that the Secretary, acting through the Director, determines necessary to help Congress understand the progress towards, and obstacles to, implementing a risk-based formula.

(B) Inapplicability of Paperwork Reduction Act

The requirements of chapter 35 of title 44 (commonly referred to as the ''Paperwork Reduction Act''), shall not apply to any action taken to carry out this paragraph.

(5) Tribal cybersecurity needs report

Not later than 2 years after November 15, 2021, the Secretary, acting through the Director, shall submit to Congress a report that—

(A) describes the cybersecurity needs of Tribal governments, which shall be determined in consultation with the Secretary of the Interior and Tribal governments; and

(B) includes any recommendations for addressing the cybersecurity needs of Tribal governments, including any necessary modifications to the State and Local Cybersecurity Grant Program to better serve Tribal governments.

(6) GAO review

Not later than 3 years after November 15, 2021, the Comptroller General of the United States shall conduct a review of the State and Local Cybersecurity Grant Program, including—

(A) the grant selection process of the Secretary; and

(B) a sample of grants awarded under this section.

(r) Authorization of appropriations

(1) In general

There are authorized to be appropriated for activities under this section—

(A) for fiscal year 2022, $200,000,000;

(B) for fiscal year 2023, $400,000,000;

(C) for fiscal year 2024, $300,000,000; and

(D) for fiscal year 2025, $100,000,000.

(2) Transfers authorized

(A) In general

During a fiscal year, the Secretary or the head of any component of the Department that administers the State and Local Cybersecurity Grant Program may transfer not more than 5 percent of the amounts appropriated pursuant to paragraph (1) or other amounts appropriated to carry out the State and Local Cybersecurity Grant Program for that fiscal year to an account of the Department for salaries, expenses, and other administrative costs incurred for the management, administration, or evaluation of this section.

(B) Additional appropriations

Any funds transferred under subparagraph (A) shall be in addition to any funds appropriated to the Department or the components described in subparagraph (A) for salaries, expenses, and other administrative costs.

(s) Termination

(1) In general

Subject to paragraph (2), the requirements of this section shall terminate on September 30, 2025.

(2) Exception

The reporting requirements under subsection (q) shall terminate on the date that is 1 year after the date on which the final funds from a grant under this section are expended or returned.

(Pub. L. 107–296, title XXII, § 2220A, formerly § 2218, as added Pub. L. 117–58, div. G, title VI, § 70612(a), Nov. 15, 2021, 135 Stat. 1272; renumbered § 2220A and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(viii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(K), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

REFERENCES IN TEXT

The Food and Nutrition Act of 2008, referred to in subsec. (m)(2)(C)(ii), is Pub. L. 88–525, Aug. 31, 1964, 78 Stat. 703, which is classified generally to chapter 51 (§ 2011 et seq.) of Title 7, Agriculture. For complete classification of this Act to the Code, see Short Title note set out under section 2011 of Title 7 and Tables.

AMENDMENTS

2022—Subsec. (a). Pub. L. 117–263, § 7143(b)(2)(K)(i), redesignated pars. (3), (4), and (8) to (12) as (1) to (7), respectively, and struck out former pars. (1), (2), and (5) to (7) which defined appropriate committees of Congress, cyber threat indicator, incident, information sharing and analysis organization, and information system, respectively.

Subsec. (e)(2)(B)(xiv)(II)(aa). Pub. L. 117–263, § 7143(b)(2)(K)(ii), substituted ''Information Sharing and Analysis Organization'' for ''information sharing and analysis organization''.

Subsec. (p). Pub. L. 117–263, § 7143(b)(2)(K)(iii), substituted ''appropriate congressional committees'' for ''appropriate committees of Congress''.

Subsec. (q)(4)(A). Pub. L. 117–263, § 7143(b)(2)(K)(iv), which directed amendment of subsec. (q)(4) by substituting ''appropriate congressional committees'' for ''appropriate committees of Congress'' ''in the matter preceding clause (i)'', was executed by making the substitution in the introductory provisions of subsec. (q)(4)(A), to reflect the probable intent of Congress.

2021—Pub. L. 117–81 reenacted section catchline.

§ 665h. National Cyber Exercise Program

(a) Establishment of program

(1) In general

There is established in the Agency the National Cyber Exercise Program (referred to in this section as the ''Exercise Program'') to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) Requirements

(A) In general

The Exercise Program shall be—

(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical infrastructure network resulting from a cyber incident;

(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

(B) Model exercise selection

The Exercise Program shall—

(i) include a selection of model exercises that government and private entities can readily adapt for use; and

(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

(I) conform to the requirements described in subparagraph (A);

(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

(III) provide for systematic evaluation of readiness.

(3) Consultation

In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, the Office of the National Cyber Director, cybersecurity research stakeholders, and Sector Coordinating Councils.

(b) Definitions

In this section:

(1) State

The term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

(2) Private entity

The term ''private entity'' has the meaning given such term in section 1501 of this title.

(c) Rule of construction

Nothing in this section shall be construed to affect the authorities or responsibilities of the Administrator of the Federal Emergency Management Agency pursuant to section 748 of this title.

(Pub. L. 107–296, title XXII, § 2220B, as added Pub. L. 117–81, div. A, title XV, § 1547(a), Dec. 27, 2021, 135 Stat. 2059.)

§ 665i. CyberSentry program

(a) Establishment

There is established in the Agency a program, to be known as ''CyberSentry'', to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions, upon request and subject to the consent of such owner or operator.

(b) Activities

The Director, through CyberSentry, shall—

(1) enter into strategic partnerships with critical infrastructure owners and operators that, in the determination of the Director and subject to the availability of resources, own or operate regionally or nationally significant industrial control systems that support national critical functions, in order to provide technical assistance in the form of continuous monitoring of industrial control systems and the information systems that support such systems and detection of cybersecurity risks to such industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of such owner or operator;

(2) leverage sensitive or classified intelligence about cybersecurity risks regarding particular sectors, particular adversaries, and trends in tactics, techniques, and procedures to advise critical infrastructure owners and operators regarding mitigation measures and share information as appropriate;

(3) identify cybersecurity risks in the information technology and information systems that support industrial control systems which could be exploited by adversaries attempting to gain access to such industrial control systems, and work with owners and operators to remediate such vulnerabilities;

(4) produce aggregated, anonymized analytic products, based on threat hunting and continuous monitoring and detection activities and partnerships, with findings and recommendations that can be disseminated to critical infrastructure owners and operators; and

(5) support activities authorized in accordance with section 1501 of the National Defense Authorization Act for Fiscal Year 2022.

(c) Privacy review

Not later than 180 days after December 27, 2021, the Privacy Officer of the Agency under section 652(h) of this title shall—

(1) review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including such laws governing the acquisition, interception, retention, use, and disclosure of communities; and

(2) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and