119TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
119–377

PROTECTING INFORMATION BY LOCAL LEADERS FOR AGENCY RESILIENCE ACT

NOVEMBER 12, 2025.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GARBARINO, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 5078]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 5078) to amend the Homeland Security Act of 2002 to reauthorize the State and local cybersecurity grant program of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes, having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 5078, the "Protecting Information by Local Leaders for Agency Resilience Act" or "PILLAR Act," reauthorizes and updates the State and Local Cybersecurity Grant Program (SLCGP) administered by the Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS). The SLCGP focuses on strengthening the cybersecurity and resilience of state, local, and territorial (SLT) governments' information systems and operational technology systems, including those that use artificial intelligence. The SLCGP enables DHS to support targeted cybersecurity investments to improve the capabilities of SLT government agencies that are oftentimes at the frontlines of U.S. cyber defense.

BACKGROUND AND NEED FOR LEGISLATION

Like Federal agencies, state and local governments are rich targets for cyber adversaries given the volume of sensitive personal data they house and the high cost that service disruptions and system failures would impose. However, state and local agencies often have far fewer resources and cybersecurity personnel than their Federal counterparts or similarly sized private sector entities. In the 2024 Deloitte and the National Association of Chief Information Officers (NASCIO) biennial cybersecurity report, "86% of state chief information security officers (CISOs) say their responsibilities are growing, yet more than one-third do not have a dedicated cybersecurity budget. Four of the 51 state CISOs surveyed said their state IT budgets allocate less than 1% for cybersecurity,"[1] which is far lower the Federal government or private industries, such as the financial services sector. Investing in cybersecurity before a cyberattack saves money, protects important data housed on state and local networks, and ensures state and local governments can continue to provide the important services Americans rely on. According to the "State of Ransomware in State and Local Government 2024," 98% of ransomware incidents in 2024 resulted in data encryption—an increase from 76% in 2023—and the average cost to recover from a ransomware attack was $2.83 million in 2024—an increase from $1.21 million in 2023.[2] To address this urgent national security issue, the Federal government sought to create a Federally-funded cybersecurity grant to redouble efforts with state and local governments to build robust cybersecurity defenses.

The Bipartisan Infrastructure Law (BIL), commonly referred to as the Infrastructure Investment and Jobs Act (IIJA), was signed into law in November 2021, which included a provision that would require DHS to establish the State SLCGP. The SLCGP is "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."[3]

---

[1] *2024 Deloitte-NASCIO Survey Finds States Face Growing Cybersecurity Threats, Tight Budgets,* National Association of State Chief Information Officers (September 30, 2024), https://www.nascio.org/press-releases/2024-deloitte-nascio-survey-finds-states-face-growing-cybersecurity-threats-tight-budgets/.

[2] *The State of Ransomware in State and Local Government 2024,* Sophos (August 2024), https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-government.

[3] 6 U.S.C. 665g et seq.

The program authorized one billion dollars over four years and expires on September 30, 2025.

The Government Accountability Office (GAO) conducted a statutorily required analysis of the impact of the SLCGP. They found that DHS provided nearly $172 million USD in grant allocations to 33 states and territories, funding almost 840 projects that align with the principles defined by the National Institute of Standards and Technology (NIST). These projects included developing cybersecurity policies, hiring various cybersecurity contractors, implementing multi-factor authentication (MFA), and updating existing equipment.[4] GAO solicited feedback from various participants and found that officials positively regarded the grant program.[5]

On March 19, 2025, President Donald J. Trump issued an Executive Order titled "Achieving Efficiency Through State and Local Preparedness." The Executive Order outlines that "[c]ommon sense approaches and investments by State and local governments across American infrastructure will enhance national security and create a more resilient Nation."[6] *The Protecting Information by Local Leaders for Agency Resilience (PILLAR) Act,* or H.R. 5078, fulfills this mandate to invest wisely in SLTT infrastructure by extending a successful program with updates based on extensive stakeholder feedback.

HEARINGS

The Committee held the following hearings in the 119th Congress that informed H.R. 5078:

On April 1, 2025, the Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled, "Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program." Members heard testimony from the following witnesses: Mr. Robert Huber, Chief Security Officer, Tenable, Inc.; Mr. Alan Fuller, Chief Information Officer, State of Utah; The Honorable Kevin Kramer, First Vice President, National League of Cities; Councilman, Louisville, KY; and Mr. Mark Raymond, Chief Information Officer, State of Connecticut.

On June 12, 2025, the Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled, "Security to Model: Securing Artificial Intelligence to Strengthen Cybersecurity." Members heard testimony from the following witnesses: Mr. Kiran Chinnagangannagari, Co-Founder and Chief Product and Technology Officer, Securin Inc.; Mr. Steve Faehl, U.S. Government Security Leader, Microsoft; Mr. Gareth Maclachlan, Chief Product Officer, Trellix; and Mr. Jonathan Dambrot, CEO, Cranium AI, Inc.

On July 22, 2025, the Committee on Homeland Security's Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled, "Fully Operational: Stuxnet 15 Years Later and the Evolution of Cyber Threats to Critical Infrastructure." Mem-

---

[4] *DHS Implemented a Grant Program to Enable State, Local, Tribal, and Territorial Governments to Improve Security,* Government Accountability Office (April 2025), https://files.gao.gov/reports/GAO-25-107313/index.html#_Toc196309939.

[5] Id.

[6] *Achieving Efficiency Through State and Local Preparedness,* The White House (Mar. 19, 2025), https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/.

bers heard testimony from the following witnesses: Ms. Kim Zetter, Journalist and Author of "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon"; Mr. Robert M. Lee, CEO and Co-Founder, Dragos Inc.; Ms. Tatyana Bolton, Executive Director, Operational Technology Cyber Coalition (OTCC); and Dr. Nathaniel Gleason, Program Leader, Lawrence Livermore National Laboratory.

COMMITTEE CONSIDERATION

The Committee met on September 3, 2025, a quorum being present, to consider H.R. 5078 and ordered the measure to be favorably reported to the House by a recorded vote of 21 yeas to 1 nay.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

COMMITTEE ON HOMELAND SECURITY 119TH CONGRESS		
Date: September 3, 2025 **Roll Call Vote No. 51**		
Ordering H.R. 5078 to be favorably reported to the House		
Yeas		**Nays**
X	Mr. McCaul, Texas	
X	Mr. Guest, Mississippi	
X	Mr. Gimenez, Florida	
X	Mr. Pfluger, Texas	
	Ms. Greene, Georgia	
X	Mr. Gonzales, Texas	
X	Mr. Luttrell, Texas	
	Mr. Strong, Alabama	
	Mr. Brecheen, Oklahoma	X
X	Mr. Crane, Arizona	
X	Mr. Ogles, Tennessee	
X	Mrs. Biggs, South Carolina	
X	Mr. Evans, Colorado	
X	Mr. Mackenzie, Pennsylvania	
	Mr. Knott, North Carolina	
X	*Mr. Thompson, Mississippi, Ranking Member*	
	Mr. Swalwell, California	
	Mr. Correa, California	
X	*Mr. Thanedar, Michigan*	
	Mr. Magaziner, Rhode Island	
X	*Mr. Goldman, New York*	
X	*Mrs. Ramirez, Illinois*	
X	*Mr. Kennedy, New York*	
X	*Mrs. McIver, New Jersey*	
X	*Ms. Johnson, Texas*	
X	*Mr. Hernández, Puerto Rico*	
	Ms. Pou, New Jersey	
X	*Mr. Carter, Louisiana*	
	Mr. Green, Texas	
X	Mr. Garbarino, New York, Chairman	
21	**TOTAL**	1

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures contained in the cost estimate prepared by the Director of the Congressional Budget Office.

H.R. 5078, Protecting Information by Local Leaders for Agency Resilience Act

As ordered reported by the House Committee on Homeland Security on September 3, 2025

By Fiscal Year, Millions of Dollars	2025	2025-2030	2025-2035
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	869	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2036?	No	Statutory pay-as-you-go procedures apply?	No
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2036?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

H.R. 5078 would extend until 2035 the requirements for the Department of Homeland Security (DHS) to make cybersecurity grants to state and local entities, assess grant applications, review state and local cybersecurity plans, and monitor the performance of grant recipients. H.R. 5078 also would expand the scope of the grant program to include state and local government investments in artificial intelligence systems. Finally, the bill would require the Comptroller General of the United States to periodically review the program. The requirement to make cybersecurity grants currently expires on September 30, 2025.

The costs of the legislation, detailed in Table 1, fall within budget function 450 (Community and Regional Development). For this estimate, CBO assumes that H.R. 5078 will be enacted near the start of fiscal year 2026 and that outlays will follow historical spending patterns for the affected programs. Implementing H.R. 5078 would cost $869 million over the 2025–2030 period, CBO estimates; such spending would be subject to the availability of appropriated funds.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 5078

	By fiscal year, millions of dollars—						
	2025	2026	2027	2028	2029	2030	2025–2030
Cybersecurity Grants:							
Estimated Authorization	0	250	250	250	250	250	1,250
Estimated Outlays	0	50	103	160	210	243	766
Management and Oversight Costs:							
Estimated Authorization	0	20	20	21	21	21	103
Estimated Outlays	0	20	20	21	21	21	103
Total Changes:							
Estimated Authorization	0	270	270	271	271	271	1,353
Estimated Outlays	0	70	123	181	231	264	869

Over the 2022–2025 period, lawmakers provided an average of $250 million per year for the DHS State and Local Cybersecurity Grant Program. CBO estimates that continuing to award grants at that level would cost $766 million over the 2025–2030 period.

On the basis of the costs to administer a similar grant program, CBO estimates that reviewing grant applications and cybersecurity plans, disbursing grants, communicating with state and local governments, and completing other oversight and administrative functions required by the bill would cost $103 million over the 2025–2030 period.

On the basis of the costs of similar reviews, CBO estimates that the cost of the periodic review by the Comptroller General would be less than $500,000 over the 2025–2030 period.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Christina Hawley Anthony, Deputy Director of Budget Analysis.

MARK P. HADLEY
(For Phillip L. Swagel, Director, Congressional Budget Office).

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act of 1995.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 5078 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 5078 is to reauthorize and update the State and Local Cybersecurity Grant Program, and for other purposes.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that H.R. 5078 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section states that the Act may be cited as the "Protecting Information by Local Leaders for Agency Resilience Act" or the "PILLAR Act."

Section 2. Reauthorization of CISA State and Local Cybersecurity Grant Program

This section amends Section 2220A of the Homeland Security Act of 2002, Reauthorization of CISA State and Local Cybersecurity Grant Program, Subsections (a), (b), (d), (e), (g), (i), (j), (l), (m), (n), (o), (p), (q), (r), (s), and (t). H.R. 5078 reauthorizes and updates the SLCGP, which is managed by CISA and FEMA of DHS. This legislation authorizes the SLCGP for ten years, subject to the availability of appropriations. The longer authorization timeline encourages long-term cybersecurity resource planning by SLTT entities and updates the bill language to capture operational technology (OT) and artificial intelligence (AI). H.R. 5078 also stabilizes the cost share over the course of the grant and incentivizes implementation of Multi-Factor Authentication (MFA) across critical infrastructure by increasing the Federal cost share. As nation-state adversaries and cybercriminals continue to target state and local entities, H.R. 5078 provides necessary resources to bolster SLTT cyber defense capabilities.

In subsection (e), there are sixteen provisions listed to drive cybersecurity risk assessment and mitigation at the SLTT level. During the April 1, 2025 hearing entitled, "Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program," witnesses testified that the cybersecurity plan requirements were helpful for recipients to target the vulnerabilities found in critical networks and services and that the statute requirements should not change. The Committee updated cybersecurity planning language to ensure that plans capture OT systems and AI, in addition to information systems. Additionally, while the grant program made strides in information sharing and identifying cyber risk, the Committee wants to encourage information sharing between Federal and state partners, including with DHS State, Local, and Re-

gional Fusion Centers, as applicable. As we have seen time and again, State Administrative Agencies (SAA) need timely intelligence from Federal partners to make meaningful, high-value decisions about where to invest limited resources or to respond to time-sensitive incidents. In addition to Federal partners, the Committee encourages consultation with information sharing and analysis organizations; small communities, regardless of whether they are rural; and academic and nonprofit entities, including cybersecurity clinics and other nonprofit technical assistance programs, as applicable. These partnerships ensure that targeted resources go to the communities who need cybersecurity assistance most.

Importantly, the bill requires an SAA to address in its Cybersecurity Plans how it will assume the cost or partial cost of cybersecurity investments made due to implementation of its plan. The Committee recognizes the challenges associated with having SLTT governments pick up the full costs of their cybersecurity needs, especially against well-funded nation-state adversaries. However, to be good stewards of Federal funding, SLTT governments need to plan on how they would assume the costs of cybersecurity if the grant were to expire. SLTT governments could pursue public-private partnerships, additional state funding, or other creative mechanisms to continue to achieve cybersecurity planning goals.

The Committee is also aware that AI is creating significant efficiencies for state and local governments, including by identifying waste, fraud, and abuse; more efficiently delivering of government services; and supporting law enforcement activities. The Committee supports these efforts to infuse innovative new technologies into legacy processes. However, like any new and rapidly evolving technology, AI requires additional focus from cybersecurity professionals as it is integrated into our digital infrastructure. This escalation of rapid AI use, novel AI code, and increasing complexity of our information systems and OT systems pose very real risks for cybersecurity systems and processes. Therefore, states and localities are encouraged to leverage these grants to manage their AI security posture, mitigate AI risk, and enhance AI system resilience against attacks. This includes continuously inventorying and evaluating AI components within broader information systems and OT systems for potential vulnerabilities.

To encourage more multi-entity grant applications found in subsection (f), the Committee urges SAAs to consider multi-entity approaches within the jurisdiction of an SAA during the Cybersecurity Planning process. For example, multiple counties may want to offer the same service or capability to their citizens. To avoid duplication and ensure resources are spent effectively, they should coordinate to pursue a multi-entity grant through their SAA. The Committee anticipates that CISA, the subject-matter expert agency, will provide additional guidance on what qualifies as a multi-entity grant within an SAA.

In subsection (g), "low or otherwise limited operating budgets'" are at the discretion of CISA to provide a framework for identifying rural, suburban, and high-population jurisdictions with significant resource limitations within an eligible entity. This language ensures that State Planning Committees understand and consider the needs of entities with the lowest capacity into their planning and investments.

The Federal government has an obligation to the American taxpayer that any technology or services purchased using taxpayer dollars follow the highest security standards available. In subsection (j)(1)(F) and (j)(1)(G), the new subparagraphs ensure state governments align with these standards as well. The Committee encourages SAAs to purchase technology or services that adhere to Secure by Design principles or other relevant and/or forthcoming guidance from CISA. Additionally, SAAs must ensure they are not buying from foreign entities of concern, as defined by those found in *42 U.S.C. 19237*.

After receiving input from stakeholders, the language in subsection (m)(1) was amended to "activities" to encourage an overall match for each grant to a state/territory, instead of a project-by-project match, which is a challenge for small, local governments. The bill also stabilizes the cost share at 60% for single entities and 70% for multi-entity groups, which is the current authorization level for Fiscal Year 2025, to make it easier for entities to plan out their investments.

Recognizing that not all Multi-Factor Authentication is created equal, the Committee expects that CISA will determine which standard of MFA-enabled or implemented on critical infrastructure that is within the entity or multi-entities' jurisdiction will qualify for the increased Federal cost share incentive laid out in subparagraph (B). The Committee recommends phishing-resistant at a minimum but included broader language to encourage the most current MFA that relies on the Fast Identity Online (FIDO) standard. The Committee defers to SLTT governments to determine their critical infrastructure, and to CISA to determine if SLTT governments have fulfilled the requirement for the increased cost share. However, the Committee's interpretation of critical infrastructure under state and local jurisdiction includes vital community services like local transportation networks, water and wastewater systems, local emergency services, and community facilities that support public safety, health, and the economy. These are distinct from Federal systems and are essential for the daily functioning of a city or town, encompassing the physical and virtual systems necessary for a region to thrive, with specific examples including municipal dams, transit systems, and local power distribution.

In subsection (n)(2)(A), the updated language alleviates the administrative burden on SAAs that were previously required to request yearly consent from all of their SLTT government partners for a given project. Under this bill, a project only requires consent once to qualify for the shared services passthrough.

Additionally, "shared services'" language in clauses (ii) and (iii) found in subparagraphs (A) and (B) is codified for SAAs to qualify for the grant passthrough requirements. A "whole-of-state" approach, whereby states provide shared services to local governments using Federal grant funding, is an encouraged approach to ensure that states provide essential cybersecurity services, such as security awareness training, endpoint detection, and exercises that would otherwise be out of reach for smaller communities. The Committee encourages SAAs to consider services that benefit the communities who need cybersecurity services the most. If a certain percentage, as determined by CISA, of localities within a state do not

opt into the shared services provided, the localities should receive direct funding from SAAs in the following fiscal year.

In paragraph (5), the Committee clarified that if direct funding is not distributed to a local government within 60 days of the anticipated grant disbursement date, the local government may petition the Secretary to receive funds directly. This provision provides more accountability for SAAs to distribute direct funding within a specified timeframe and enables local governments to apply directly for funding if the SAA is not in compliance with the terms of the grant—something that came up during the Committee's April 1, 2025 hearing entitled, "Cybersecurity is Local, Too: Assessing the State and Local Cybersecurity Grant Program."

The Committee added language in subsection (o) to include representatives from local governments with small populations to ensure they are consulted during the Cybersecurity Plan development process. This would fulfill a primary goal of this bill, which is to help the communities that need to improve their cyber posture most. The new subsection (p) also encourages DHS outreach to local governments with small populations to inform them about no-cost cybersecurity service offerings available from CISA.

Subsection (r) directs GAO to provide a review of the grant program every four years to ensure that the program is following the intent of Congress. GAO will also review the grant program to evaluate the adoption of AI by SAAs in their Cybersecurity Plans.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE.—The term "artificial intelligence" has the meaning given such term in section 5002(3) of the National Artificial Intelligence Initiative Act of 2020 (enacted as division E of the William M. (Mac) Thornberry Na-

tional Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 9401(3))).

(2) ARTIFICIAL INTELLIGENCE SYSTEM.—The term "artificial intelligence system" means any data system, software, hardware, application tool, or utility that operates in whole or in part using artificial intelligence.

[(1)**]** *(3)* CYBERSECURITY PLAN.—The term "Cybersecurity Plan" means a plan submitted by an eligible entity under subsection (e)(1).

[(2)**]** *(4)* ELIGIBLE ENTITY.—The term "eligible entity" means a—

(A) State; or

(B) Tribal government.

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

[(3)**]** *(6)* MULTI-ENTITY GROUP.—The term "multi-entity group" means a group of 2 or more eligible entities desiring a grant under this section.

(7) MULTI-FACTOR AUTHENTICATION.—The term "multi factor authentication" means an authentication system that requires more than one distinct type of authentication factor for successful authentication of a user, including by using a multi-factor authenticator or by combining single-factor authenticators that provide different types of factors.

[(4)**]** *(8)* ONLINE SERVICE.—The term "online service" means any internet-facing service, including a website, email, virtual private network, or custom application.

[(5)**]** *(9)* RURAL AREA.—The term "rural area" has the meaning given the term in section 5302 of title 49, United States Code.

[(6)**]** *(10)* STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term "State and Local Cybersecurity Grant Program" means the program established under subsection (b).

[(7)**]** *(11)* 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 104 of the Federally Recognized Indian Tribe List Act of 1994 (25 U.S.C. 5131).

(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**]** *information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or* 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 2003 and 2004.

(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] *to the information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or* 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] *information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or* 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, 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;]

(i) manage, monitor, and track applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, that are maintained, 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 such information systems or operational technology systems (as the case may be), including legacy information systems, operational technology systems, and information technology that are no longer supported by the manufacturer of the systems or technology at issue;

(ii) monitor, audit, and track network traffic and activity transiting or traveling to or from applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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 applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, main-

tained, 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 applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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, particularly identity and access management solutions such as multi-factor authentication, which may include—

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

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

(III) knowledge bases of adversary tools and tactics;

(IV) technologies such as artificial intelligence; and

(V) improving cyber incident response capabilities through adoption of automated cybersecurity practices;

(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 entity 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 *or operational technology systems, including either or both of such systems using artificial intelligence,* 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*, including through Department of Homeland Security State, Local, and Regional Fusion Center Initiative under section 210(A)*; and

(II) the Department;

(xii) leverage cybersecurity services offered by the Department*, including for bolstering the resilience of outdated or vulnerable information systems or operational technology systems, including either or both of such systems using artificial intelligence*;

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

(xiii) implement an information technology or operational technology, including either or both of such systems using artificial intelligence, modernization cybersecurity review process that ensures alignment between information technology, operational technology, and artificial intelligence 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; *and*

(cc) academic and nonprofit entities, including cybersecurity clinics and other nonprofit technical assistance programs;

[(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**]**

(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas and other local governments with small populations within the jurisdiction of the eligible entity, including by direct outreach to such rural areas and local governments with small populations; 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.**]**

(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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

(iii) assuming the cost or partial cost of cybersecurity investments made as a result of the plan.

(3) DISCRETIONARY ELEMENTS.—In drafting a Cybersecurity Plan, an eligible entity may—

(A) consult with **[**the Multi-State Information Sharing and Analysis Center**]** *Information Sharing and Analysis Organizations*;

(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 *including, as appropriate, representatives of rural, sub-*

urban, and high-population jurisdictions (including such jurisdictions with low or otherwise limited operating budgets); 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.]

(5) RULE OF CONSTRUCTION REGARDING CONTROL OF CERTAIN INFORMATION SYSTEMS OR OPERATIONAL TECHNOLOGY SYSTEMS OF ELIGIBLE ENTITIES.—Nothing in this subsection may 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 or operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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 Cybersecu-

rity Plan satisfies the requirements under paragraph (2), the determination shall be effective for the [2-year period] *3-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] *2027*, 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] *2027*.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection [shall] *may* 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] *information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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] *information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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[.]*;*

(E) to purchase software or hardware, or products or services of such software or hardware, as the case may be, that do not align with guidance relevant to such software or hardware, or products or services, as the case may be, provided by the Agency, including Secure by Design or successor guidance; or

(F) to purchase software or hardware, or products or services of such software or hardware, as the case may be, that are designed, developed, operated, maintained, manufactured, or sold by a foreign entity of concern and do not align with guidance provided by the Agency.

(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] *2026* 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.]

(1) IN GENERAL.—The Federal share of activities carried out using funds made available pursuant to the award of a grant under this section may not exceed—

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

(B) in the case of a grant to a multi-entity group, 70 percent for each fiscal year through fiscal year 2035.

Notwithstanding subparagraphs (A) and (B), the Federal share of the cost for an eligible entity or multi-entity group shall be 65 percent for an entity and 75 percent for a multi-group entity for each fiscal year beginning with fiscal year 2028 through fiscal year 2035 if such entity or multi-entity group entity, as the case may be, implements or enables, by not later than October 1, 2027, multi-factor authentication and identity and access management tools that support multi-factor authentication with respect to critical infrastructure, including the information systems and operational technology systems, including either or both of such systems using artificial intelligence, of such critical infrastructure, that is within the jurisdiction of such entity or multi-entity group is responsible.

(2) WAIVER.—

(A) IN GENERAL.—The Secretary may waive or modify the requirements of paragraph (1) if an eligible entity 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**]** *a grant on or after January 1, 2026, or changes the allocation of funding as permissible within the allowances of* 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.**]**

(ii) with the consent of the local governments, items, in-kind services, capabilities, or activities, or a combination of funding and other services, 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, in-kind services, capabilities, or activities, or a combination of funding and other services, 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.**]**

(ii) items, in kind services, capabilities, or activities, or a combination of funding and other services, 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, in kind services, capabilities, or activities, or a combination of funding and other services, 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.]

(5) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local government required under paragraph (2) within 60 days of the anticipated grant disbursement date, such local government may petition the Secretary to request the Secretary to provide funds directly to such local government.

(6) LIMITATION ON CONSTRUCTION.—A grant awarded under this section may not be used to acquire land or to construct, remodel, 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 *and representatives from rural areas and other local governments with small populations*, 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) OUTREACH TO LOCAL GOVERNMENTS.—The Secretary, acting through the Director, shall implement an outreach plan to inform local governments, including those in rural areas or with small populations, about no-cost cybersecurity service offerings available from the Agency.

[(p)] *(q)* 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)] *(r)* 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] *information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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*

(iii) assuming the costs associated with continuing the programs specified in the Cybersecurity Plan by including such programs in State and local government budgets upon full expenditure of grant funds by 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] *information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, 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, United States Code (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, United States Code (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 the date of enactment of this section, 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 the date of enactment of this section, 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.]

(6) GAO REVIEW.—Not later than four years after the date of the enactment of this paragraph and every four years thereafter until the termination of the State and Local Cybersecurity Grant Program, the Comptroller General of the United States shall conduct a review of the Program, including relating to the following:

(A) The grant selection process of the Secretary.

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

(C) A review of artificial intelligence adoption across the sample of grants reviewed.

[(r)] *(s)* 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.]

(1) IN GENERAL.—The activities under this section are subject to the availability of appropriations.

(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)] *(t)* TERMINATION.—

(1) IN GENERAL.—Subject to paragraph (2), the requirements of this section shall terminate on September 30, [2025] *2035*.

(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.

* * * * * * *

○