3.1.2 Establish a National Cyber Resilience Assistance Fund

This proposal establishes a National Cyber Resilience Assistance Fund for projects and programs aimed at systematically increasing the resilience of public and private entities, thereby increasing the overall resilience of the United States.

A BILL

To establish a National Cyber Resilience Assistance Fund for projects and programs aimed at systematically increasing the resilience of public and private entities in the United States, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. SHORT TITLE.

This Act may be cited as the "National Cyber Resilience Assistance Fund Act".

SEC. 2. ESTABLISHMENT OF THE NATIONAL CYBER RESILIENCE ASSISTANCE FUND.

"(a) Definitions.—In this section:

"(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given that term in section 2209.

"(2) ELIGIBLE ENTITY.—The term 'eligible entity' means an entity that meets the guidelines and requirements for eligible entities established by the Secretary under subsection (d)(4).

"(3) FUND.—The term 'Fund' means the National Cyber Resilience Assistance Fund established under subsection (c).

"(4) NATIONAL CRITICAL FUNCTIONS.—The term 'national critical functions' means the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

"(b) Creation of a Critical Infrastructure Resilience Strategy and a National Risk Management Cycle.—

"(1) INITIAL RISK IDENTIFICATION AND ASSESSMENT.—

"(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, vulnerabilities, and consequences.

"(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall coordinate with the heads of Sector Risk Management Agencies and the National Cyber Director and consult with critical infrastructure owners and

operators.

"(C) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A).

"(D) REPORT.—Not later than 1 year after the date of enactment of this section, the Secretary shall submit to the President, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the risks identified by the process established under subparagraph (A).

"(2) INITIAL NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

"(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers the report required under paragraph (1)(D), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

"(B) ELEMENTS.—In the strategy delivered under subparagraph (A), the President shall—

"(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise, disrupt, or impede the ability of the critical infrastructure to support the national critical functions of national security, economic security, or public health and safety;

"(ii) identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified;

"(iii) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each;

"(iv) outline the budget plan required to provide sufficient resources to successfully execute the full range of activities proposed or described by the strategy; and

"(v) request any additional authorities or resources necessary to successfully execute the strategy.

"(C) FORM.—The strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

"(3) ANNUAL REPORTS.—

"(A) IN GENERAL.—Not later than 1 year after the date on which the President delivers the strategy under paragraph (2), and every year thereafter, the Secretary, in coordination with the heads of Sector Risk Management Agencies, shall submit to the appropriate congressional committees a report on the national risk management cycle activities undertaken pursuant to the strategy, including—

"(i) all variables included in risk assessments and the weights assigned to each such variable;

"(ii) an explanation of how each such variable, as weighted, correlates to risk, and the basis for concluding there is such a correlation; and

"(iii) any change in the methodologies since the previous report under this paragraph, including changes in the variables considered, weighting of those variables, and computational methods.

"(B) CLASSIFIED ANNEX.—The reports required under subparagraph (A) shall be submitted in unclassified form to the greatest extent possible, and may include a classified annex if necessary.

"(4) FIVE YEAR RISK MANAGEMENT CYCLE.—

"(A) RISK IDENTIFICATION AND ASSESSMENT.—Under procedures established by the Secretary, the Secretary shall repeat the conducting and reporting of the risk identification and assessment required under paragraph (1), in accordance with the requirements in paragraph (1), every 5 years.

"(B) STRATEGY.—Under procedures established by the President, the President shall repeat the preparation and delivery of the critical infrastructure resilience strategy required under paragraph (2), in accordance with the requirements in paragraph (2), every 5 years, which shall also include assessing the implementation of the previous national critical infrastructure resilience strategy.

"(c) Establishment of the National Cyber Resilience Assistance Fund.—There is established in the Treasury of the United States a fund, to be known as the 'National Cyber Resilience Assistance Fund', which shall be available for the cost of risk-based grant programs focused on systematically increasing the resilience of public and private critical infrastructure against cybersecurity risk, thereby increasing the overall resilience of the United States.

"(d) Administration of Grants From the National Cyber Resilience Assistance Fund.—

"(1) IN GENERAL.—In accordance with this section, the Secretary, acting through the Administrator of the Federal Emergency Management Agency and the Director, shall develop and administer processes to—

"(A) establish focused grant programs to address identified areas of cybersecurity risk to, and bolster the resilience of, critical infrastructure;

"(B) accept and evaluate applications for each such grant program;

"(C) award grants under each such grant program; and

"(D) disburse amounts from the Fund.

"(2) ESTABLISHMENT OF RISK-FOCUSED GRANT PROGRAMS.—

"(A) ESTABLISHMENT.—

"(i) IN GENERAL.—The Secretary, acting through the Director and the Administrator of the Federal Emergency Management Agency, may establish not less than 1 grant program focused on mitigating an identified category of cybersecurity risk identified under the national risk management cycle and critical

infrastructure resilience strategy under subsection (b) in order to bolster the resilience of critical infrastructure within the United States.

"(ii) SELECTION OF FOCUS AREA.—Before selecting a focus area for a grant program pursuant to this subparagraph, the Director shall ensure—

"(I) there is a clearly-defined cybersecurity risk identified through the national risk management cycle and critical infrastructure resilience strategy under subsection (b) to be mitigated;

"(II) market forces do not provide sufficient private-sector incentives to mitigate the risk without Government investment; and

"(III) there is clear Federal need, role, and responsibility to mitigate the risk in order to bolster the resilience of critical infrastructure.

"(B) FUNDING.—

"(i) RECOMMENDATION.—Beginning in the first fiscal year following the establishment of the Fund and each fiscal year thereafter, the Director shall—

"(I) assess the funds available in the Fund for the fiscal year; and

"(II) recommend to the Secretary the total amount to be made available from the Fund under each grant program established under this subsection.

"(ii) ALLOCATION.—After considering the recommendations made by the Director under clause (i) for a fiscal year, the Director shall allocate amounts from the Fund to each active grant program established under this subsection for the fiscal year.

"(3) USE OF FUNDS.—

"(A) IN GENERAL.—Amounts in the Fund shall be used by the Director to proactively mitigate risks identified through the national risk management cycle and critical infrastructure resilience strategy under subsection (b) before cyber incidents occur, through activities such as—

"(i) proactive vulnerability assessments and mitigation;

"(ii) defrayal of costs to invest in backup systems critical to mitigating national or economic security risks, as determined by the Federal Government, with cost-sharing from the recipient entity in accordance with subparagraph (B);

"(iii) defrayal of costs to invest in replacing vulnerable systems and assets critical to mitigating national or economic security risks, as determined by the Federal Government, with more secure alternatives, with cost-sharing from the recipient entity in accordance with subparagraph (B);

"(iv) grants to nonprofit entities to develop publicly available low-cost or no-cost cybersecurity tools for small-sized and medium-sized entities;

"(v) proactive threat detection and hunting; and

"(vi) network protections.

"(B) FEDERAL SHARE.—The Federal share of the cost of an activity described in

clause (ii) or (iii) of subparagraph (A) that is carried out using funds made available under this section may not exceed—

"(i) for fiscal year 2022, 90 percent;

"(ii) for fiscal year 2023, 80 percent;

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

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

"(v) for fiscal year 2026, and each fiscal year thereafter, 50 percent.

"(4) ELIGIBLE ENTITIES.—

"(A) GUIDELINES AND REQUIREMENTS.—

"(i) IN GENERAL.—In accordance with this subparagraph, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a set of guidelines and requirements for determining the entities that are eligible entities.

"(ii) TYPES OF ENTITIES.—The following entities shall be eligible to receive grants using amounts in the Fund:

"(I) A State, local, tribal or territorial government.

"(II) A public owner or operator of critical infrastructure.

"(III) A private owner or operator of critical infrastructure.

"(iii) LIMITATION.—No entity shall be eligible to receive more than 1 grant under each grant program established under the Fund in any fiscal year.

"(iv) DEADLINES.—The Secretary shall submit the guidelines and requirements under clause (i)—

"(I) not later than 180 days after the date of enactment of this section, and every 2 years thereafter; and

"(II) not later than 90 days before the date on which the Secretary implements the guidelines and requirements.

"(B) CONSIDERATIONS.—In developing guidelines and requirements for eligible entities under subparagraph (A), the Secretary shall consider—

"(i) number of employees;

"(ii) annual revenue;

"(iii) existing entity cybersecurity spending;

"(iv) current cyber risk assessments, including credible threats, vulnerabilities, and consequences; and

"(v) entity capacity to invest in mitigating cybersecurity risk absent assistance from the Federal Government.

"(5) LIMITATION.—For any fiscal year, an eligible entity may not receive more than 1 grant from each grant program established under this subsection.

"(6) GRANT PROCESSES.—The Secretary, acting through the Administrator of the Federal Emergency Management Agency, shall require the submission of such information as the Secretary determines is necessary to—

"(A) evaluate a grant application against the criteria established under this section;

"(B) disburse grant funds;

"(C) provide oversight of disbursed grant funds; and

"(D) evaluate the effectiveness of the funded project in increasing the overall resilience of the United States with respect to cybersecurity risks.

"(7) GRANT CRITERIA.—For each grant program established under this subsection, the Director, in coordination with the Administrator of the Federal Emergency Management Agency and the heads of appropriate Sector Risk Management Agencies, shall develop and publish criteria for evaluating applications for funding, which shall include—

"(A) whether the application identifies a clearly-defined cybersecurity risk;

"(B) whether the cybersecurity risk identified in the grant application poses a substantial threat to critical infrastructure;

"(C) whether the application identifies a program or project clearly designed to mitigate a cybersecurity risk;

"(D) the potential consequences of leaving the identified cybersecurity risk unmitigated, including the potential impact to the critical functions and overall resilience of the nation; and

"(E) other appropriate factors identified by the Director.

"(8) EVALUATION OF GRANTS APPLICATIONS.—

"(A) IN GENERAL.—Utilizing the criteria established under paragraph (7), the Director, in coordination with the Administrator of the Federal Emergency Management Agency and the heads of appropriate Sector Risk Management Agencies, shall evaluate grant applications made under each grant program established under this subsection.

"(B) RECOMMENDATION.—Following the evaluations required under subparagraph (A), the Director shall recommend to the Secretary applications for approval, including the amount of funding recommended for each such approval.

"(9) AWARD OF GRANT FUNDING.—The Secretary shall—

"(A) review the recommendations of the Director prepared pursuant to paragraph (8);

"(B) provide a final determination of grant awards to the Administrator of the Federal Emergency Management Agency to be disbursed and administered under the process established under paragraph (6); and

"(C) provide the heads of Sector Risk Management Agencies with notice of the

eligible entities receiving grant awards under this section and the intended uses of funds disbursed under the grants.

"(e) Evaluation of Grant Programs Utilizing the National Cyber Resilience Assistance Fund.—

"(1) EVALUATION.—The Secretary shall establish a process to evaluate the effectiveness and efficiency of grants distributed under this section and develop appropriate updates, as needed, to the grant programs.

"(2) ANNUAL REPORT.—Not later than 180 days after the conclusion of the first fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a report detailing the grants awarded from the Fund, the status of projects undertaken with the grant funds, any planned changes to the disbursement methodology of the Fund, measurements of success, and total outlays from the Fund.

"(3) GRANT PROGRAM REVIEW.—

"(A) ANNUAL ASSESSMENT.—Before the start of the second fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Director shall assess the grant programs established under this section and determine—

"(i) for the coming fiscal year—

"(I) whether new grant programs with additional focus areas should be created;

"(II) whether any existing grant program should be discontinued; and

"(III) whether the scope of any existing grant program should be modified; and

"(ii) the success of the grant programs in the prior fiscal year.

"(B) SUBMISSION TO CONGRESS.—Not later than 90 days before the start of the second fiscal year in which grants are awarded under this section, and every fiscal year thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives the assessment conducted pursuant to subparagraph (A) and any planned alterations to the grant program for the coming fiscal year.

"(f) Limitation on Use of Grant Funds.—Funds awarded pursuant to this section—

"(1) shall supplement and not supplant State or local funds or, as applicable, funds supplied by the Bureau of Indian Affairs; and

"(2) may not be used—

"(A) to provide any Federal cost-sharing contribution on behalf of a State or local government;

"(B) to pay a ransom;

"(C) by or for a non-United States entity; or

"(D) for any recreational or social purpose.

"(g) Authorization of Appropriations.—There are authorized to be appropriated to carry out this section $75,000,000 for each of fiscal years 2022 through 2026.

"(h) Transfers Authorized.—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 subsection (g) or other amounts appropriated to carry out the National Cyber Resilience Assistance Fund 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.

"(i) Government Accountability Office Report.—Not later than 2years after the date of the enactment of this section, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs in the Senate and the Committee on Homeland Security in the House of Representatives a report containing the results of a study regarding the effectiveness of the programs described in this section.".

(b) Technical and Conforming Amendments.—

(1) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

"Sec.2214.National Asset Database.

"Sec.2215.Duties and authorities relating to .gov internet domain.

"Sec.2216.Joint Cyber Planning Office.

"Sec.2217.Cybersecurity State Coordinator.

"Sec.2218.Sector Risk Management Agencies.

"Sec.2219.Cybersecurity Advisory Committee.

"Sec.2220.Cybersecurity education and training programs.

"Sec.2220A.National Cyber Resilience Assistance Fund.".

(2) ADDITIONAL TECHNICAL AMENDMENT.—

(A) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking "Homeland Security Act" and inserting "Homeland Security Act of 2002".

(B) EFFECTIVE DATE.—The amendment made by subparagraph (A) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).