.....

(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. _____

To direct the Secretary of the Treasury to submit a report on coordination in the public and private sectors in responding to ransomware attacks on financial institutions, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. NUNN of Iowa introduced the following bill; which was referred to the Committee on _____

A BILL

To direct the Secretary of the Treasury to submit a report on coordination in the public and private sectors in responding to ransomware attacks on financial institutions, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Public and Private Sector Ransomware Response Coordination Act of 2024''.

SEC. 2. REPORT ON COORDINATION IN THE PUBLIC AND PRIVATE SECTORS IN RESPONDING TO RANSOMWARE ATTACKS ON FINANCIAL INSTITUTIONS.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this section, the Secretary of the Treasury shall submit to the appropriate congressional committees a report that describes the following:

(1) The current level of coordination and collaboration between the public and private sectors, including entities in the public and private sectors that manage cybersecurity, in response to, and for the prevention of, a ransomware attack on a financial institution.

(2) The coordination among relevant governmental agencies in response to, and for the prevention of, a ransomware attack on a financial institution.

(3) Whether relevant governmental agencies have timely access to relevant information reported by a financial institution following a ransomware attack on the financial institution.

(4) The utility of such information to any relevant governmental agency in the prevention or investigation of a ransomware attack on a financial in-

stitution, or the prosecution of a person responsible for such attack.

(5) An analysis of reporting requirements applicable to a financial institution with respect to a ransomware attack in relation to the utility to any relevant governmental agency of the reported information in the prevention or investigation of a ransomware attack on a financial institution, or the prosecution of a person responsible for such attack.

(6) Whether further legislation is required to increase the utility and timely access of such information to any relevant governmental agency following a ransomware attack on a financial institution.

(7) Any recommended policy initiatives to bolster public-private partnerships, increase incident report sharing, and decrease incident response time.

(8) The extent to which, and reasons that, financial institutions withhold or delay reporting to relevant governmental agencies information about a ransomware attack.

(9) Any feedback on the contents of the report received from cybersecurity and ransomware response entities that provide services to financial institutions.

(b) FORM OF REPORT.—The report described in subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(c) BRIEFING.—Not later than 15 months after the date of the enactment of this section, the Secretary of the Treasury shall brief the appropriate congressional committees on the findings of the report described in subsection (a).

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Financial Services of the House of Representatives;

(B) the Permanent Select Committee on Intelligence of the House of Representatives;

(C) the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(D) the Select Committee on Intelligence of the Senate.

(2) CYBERSECURITY AND RANSOMWARE INCIDENT RESPONSE ENTITY.—The term ''cybersecurity and ransomware incident response entity'' means an entity that provides incident responses, managed services, or advisory services that—

(A) supports investigation and risk management related to ransomware attacks in the public and private sectors;

(B) strengthens cybersecurity technology in the financial sector; and

(C) reduces overall cyber risk in the financial sector by assessing the security posture of a financial institution, assisting a financial institution with regulatory compliance, and providing recommendations to a financial institution for recovery after a ransomware attack and prevention of any future attacks.

(3) FINANCIAL INSTITUTION.—The term ''financial institution'' has the meaning given that term under section 5312(a) of title 31, United States Code.