.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to require certain coordination between the Department of Homeland Security and Federal and non-Federal entities relating to cybersecurity risks and incidents, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. TAYLOR introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Homeland Security Act of 2002 to require certain coordination between the Department of Homeland Security and Federal and non-Federal entities relating to cybersecurity risks and incidents, 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 ''Strengthening State and Local Cybersecurity Defenses Act''.

SEC. 2. COOPERATION RELATING TO CYBERSECURITY RISKS AND INCIDENTS.

Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 652 et seq. is amended—

(1) in section 2201 (6 U.S.C. 651)—

(A) by redesignating paragraphs (4), (5), and (6) as paragraphs (5), (6), and (7), respectively; and

(B) by inserting after paragraph (3) the following new paragraph:

''(4) ENTITY.—The term 'entity' includes—

''(A) an association, corporation, whether for-profit or nonprofit, partnership, proprietorship, organization, institution, establishment, or individual, whether domestic or foreign;

''(B) a government agency or other governmental entity, whether domestic or foreign, including State, local, Tribal, and territorial government entities; and

''(C) the general public.'';

(2) in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659), by adding at the end the following new subsection:

''(n) COORDINATION.—The Director shall, to the extent practicable, and in coordination as appropriate with

Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center—

''(1) conduct exercises with Federal and non-Federal entities;

''(2) provide operational and technical cybersecurity training related to cyber threat indicators, defensive measures, cybersecurity risks, and incidents to Federal and non-Federal entities to address cybersecurity risks or incidents, with or without reimbursement;

''(3) assist Federal and non-Federal entities, upon request, in sharing cyber threat indicators, defensive measures, cybersecurity risks, and incidents from and to the Federal Government as well as among Federal and non-Federal entities, in order to increase situational awareness and help prevent incidents;

''(4) provide Federal and non-Federal entities timely notifications containing specific incident and malware information that may affect such entities or individuals with respect to whom such entities have a relationship;

''(5) provide and periodically update via a web portal and other means tools, products, resources, policies, guidelines, controls, procedures, and other

cybersecurity standards and best practices and procedures related to information security;

''(6) work with senior Federal and non-Federal officials, including State and local Chief Information Officers, senior election officials, and through national associations, to coordinate a nationwide effort to ensure effective implementation of tools, products, resources, policies, guidelines, controls, procedures and other cybersecurity standards and best practices and procedures related to information security to secure and ensure the resiliency of Federal and non-Federal information systems, including election systems;

''(7) provide, upon request, operational and technical assistance to Federal and non-Federal entities to implement tools, products, resources, policies, guidelines, controls, procedures, and other cybersecurity standards and best practices and procedures related to information security, including by, as appropriate, deploying and sustaining cybersecurity technologies, such as an intrusion detection capability, to assist such Federal and non-Federal entities in detecting cybersecurity risks and incidents;

''(8) assist Federal and non-Federal entities in developing policies and procedures for coordinating

vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry;

''(9) ensure that Federal and non-Federal entities, as appropriate, are made aware of the tools, products, resources, policies, guidelines, controls, procedures, and other cybersecurity standards and best practices and procedures related to information security developed by the Department and other appropriate Federal entities for ensuring the security and resiliency of civilian information systems; and

''(10) promote cybersecurity education and awareness through engagements with Federal and non-Federal entities.''.