4.3 Establish a Bureau of Cyber Statistics

This proposal establishes a Bureau of Cyber Statistics that would act as the government statistical agency that collects, processes, analyzes, and disseminates essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other Federal agencies, State and local governments, and the private sector.

A BILL

To establish a Bureau of Cyber Statistics to collect, process, analyze, and disseminate essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other Federal agencies, State and local governments, and the private sector, 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. ESTABLISH THE BUREAU OF CYBER STATISTICS.

(a) In General.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.), as amended by section 101 of this Act, is amended by adding at the end the following:

"SEC. 2220B. BUREAU OF CYBER STATISTICS.

"(a) Definitions.—In this section:

"(1) BUREAU.—The term 'Bureau' means the Bureau of Cybersecurity Statistics established under subsection (b).

"(2) CENTER.—The term 'Center' means the Federal information security incident center described in section 3556 of title 44, United States Code.

"(3) COVERED CLAIM.—The term 'covered claim' means an insurance claim paid by a covered entity as a result of a cyber incident.

"(4) COVERED ENTITY.—The term 'covered entity' means any nongovernmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture (without regard to whether it is established for profit) that is engaged in or affecting interstate commerce and that provides cybersecurity insurance products.

"(5) CYBER INCIDENT.—The term 'cyber incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system, including the following:

"(A) Unauthorized access to an information system or network that leads to loss of confidentiality, integrity, or availability of that information system or network.

"(B) Disruption of business operations due to a distributed denial of service attack against an information system or network.

"(C) Unauthorized access or disruption of business operations due to loss of service facilitated through, or caused by a cloud service provider, managed service provider, or other data hosting provider.

"(D) Fraudulent or malicious use of a cloud service account, data hosting account, internet service account, or any other digital service.

"(6) EXECUTIVE ASSISTANT DIRECTOR.—The term 'Executive Assistant Director' means the Director of the Bureau.

"(7) STATISTICAL PURPOSE.—The term 'statistical purpose'—

"(A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and

"(B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subsection (f).

"(b) Establishment.—There is established within the Agency a Bureau of Cybersecurity Statistics.

"(c) Executive Assistant Director.—

"(1) IN GENERAL.—The Bureau shall be headed by a Director, who shall—

"(A) have a rank equivalent to an assistant secretary of the Department;

"(B) be appointed by the President; and

"(C) report to the Director.

"(2) AUTHORITY.—The Executive Assistant Director shall—

"(A) have final authority for all cooperative agreements and contracts awarded by the Bureau;

"(B) be responsible for the integrity of data and statistics collected or issued by the Bureau; and

"(C) protect against improper or illegal use or disclosure of information furnished for exclusively statistical purposes under this section, consistent with the requirements of subsection (g).

"(3) QUALIFICATIONS.—The Executive Assistant Director—

"(A) shall have experience in statistical programs; and

"(B) shall not—

"(i) engage in any other employment; or

"(ii) hold any office in, or act in any capacity for, any organization, agency, or institution with which the Bureau makes any contract or other arrangement under this section.

"(4) DUTIES AND FUNCTIONS.—The Executive Assistant Director shall—

"(A) collect and analyze information concerning cybersecurity, including data

related to cyber incidents, cyber crime, and any other area the Executive Assistant Director determines appropriate;

"(B) collect and analyze data that will serve as a continuous and comparable national indication of the prevalence, incidents, rates, extent, distribution, and attributes of all relevant cyber incidents, as determined by the Executive Assistant Director, in support of national policy and decision making;

"(C) compile, collate, analyze, publish, and disseminate uniform national cyber statistics concerning any area that the Executive Assistant Director determines appropriate;

"(D) in coordination with the National Institute of Standards and Technology, recommend national standards, metrics, and measurement criteria for cyber statistics and for ensuring the reliability and validity of statistics collected pursuant to this subsection;

"(E) conduct or support research relating to methods of gathering or analyzing cyber statistics and anonymized datasets;

"(F) enter into cooperative agreements or contracts with public agencies, institutions of higher education, or private organizations for purposes related to this subsection;

"(G) provide appropriate information to the President, the Congress, Federal agencies, the private sector, and the general public on cyber statistics;

"(H) maintain liaison with State and local governments concerning cyber statistics; and

"(I) confer and cooperate with Federal statistical agencies as needed to carry out the purposes of this section, including by entering into cooperative data sharing agreements in conformity with all laws and regulations applicable to the disclosure and use of data.

"(d) Furnishment of Information, Data, or Reports by Federal Departments and Agencies.—

"(1) DEFINITION.—In this subsection, the term 'incident' has the meaning given that term in section 3552 of title 44, United States Code.

"(2) CONSULTATION.—The Director of the Office of Management and Budget, the Secretary, and the National Cyber Director shall consult with the Executive Assistant Director with respect to the reporting of incidents.

"(3) REPORTING REQUIREMENT.—Not later than 1 year after the date of the enactment of this section, the Executive Assistant Director shall provide the Director of the Office of Management and Budget, the Secretary, and the National Cyber Director a list of data to be reported to the Center in order to develop meaningful cybersecurity statistics about the operation of Federal networks.

"(4) ANNUAL UPDATE.—The Executive Assistant Director shall update the reporting requirements described in paragraph (3) on an annual basis.

"(5) ENFORCEMENT.—The Director of the Office of Management and Budget, in consultation with the Secretary and the National Cyber Director, shall use the authority

under section 3553 of title 44, United States Code, to ensure agencies provide the data required under paragraph (3) when reporting incidents to the Center.

"(e) Furnishment of Information, Data, or Reports by State Governments.—

"(1) IN GENERAL.—The Executive Assistant Director shall request information necessary to carry out the purposes of subsection (c), including information collected through data breach reporting laws of States, from State governments.

"(2) STANDARDIZATION.—Not later than 180 days after the date of enactment of this section, and every 2 years thereafter, the Executive Assistant Director shall publish—

"(A) the information and data from State governments determined necessary to carry out the purposes of subsection (c), including information collected through state data breach reporting laws; and

"(B) common standard requirements through which States may transmit information described in subparagraph (A) to the Bureau.

"(3) GRANTS TO STATES FOR THE SUBMISSION OF DATA.—

"(A) IN GENERAL.—The Executive Assistant Director may award grants to States to assist in collecting and transmitting information to the Bureau in accordance with the standards published under paragraph (2).

"(B) APPLICATION.—Each State that desires a grant under this paragraph shall submit an application to the Executive Assistant Director at such time, in such manner, and accompanied by or containing such information as the Executive Assistant Director shall reasonably require.

"(C) DATE FOR SUBMISSION.—Applications submitted under subparagraph (B) shall be submitted during the 60-day period beginning on a date that the Executive Assistant Director shall prescribe.

"(D) DEADLINE.—An application for a grant under this paragraph shall be approved or denied by the Executive Assistant Director not later than 90 days after the date on which the Executive Assistant Director receives the application.

"(E) GRANT AMOUNT.—A grant under this paragraph shall not exceed $200,000 for any single State in any 1-year period.

"(F) REPORTING.—

"(i) COMPLIANCE.—

"(I) IN GENERAL.—Except as provided in subclauses (II) and (III), on and after the date that is 1 year after the date on which a State receives a grant under subparagraph (B), and every 3 months thereafter, the State shall submit information as specified in paragraph (2) to the Executive Assistant Director.

"(II) EXTENSIONS.—The Executive Assistant Director may provide a 90-day extension to a State that is making good faith efforts to comply with subclause (I).

"(III) NEW DATA.—If, upon a review under paragraph (2), the Executive Assistant Director publishes new data and information necessary to carry out

the purposes of subsection (c), a State shall include information relating to the new data and information in each submission under subclause (I) made by the State on or after the date that is 1 year after the date on which the Executive Assistant Director publishes the new data and information.

"(ii) FAILURE TO COMPLY.—If a State that receives a grant under subparagraph (B) fails to substantially comply with clause (i) of this subparagraph, the State shall repay the grant in full, plus reasonable interest and penalty charges allowable by law or established by the Executive Assistant Director.

"(G) BIANNUAL REPORTS.—Not later than 1 year after the date of enactment of this section, and every 2 years thereafter, the Executive Assistant Director shall submit to Congress a report describing the applications submitted for grants under this paragraph, the award of such grants, the purposes for which the grant amounts were expended, and an assessment of the effectiveness of the awarded grants in generating relevant information for the Bureau.

"(f) Furnishment of Data Related to Covered Claims.—

"(1) IN GENERAL.—Not later than 180 days after the finalization of a final rule promulgated under paragraph (7), and every 90 days thereafter, each covered entity shall submit to the Bureau a report containing such data and information about each covered claim paid in the preceding 90 day period.

"(2) DETERMINATION OF DATA AND INFORMATION NECESSARY TO CARRY OUT THE PURPOSES OF THIS SECTION.—Not later than 180 days after the date of enactment of this section, and every 180 days thereafter, the Executive Assistant Director shall publish a list of data and information determined necessary to carry out the purposes of this section, including individual descriptions of cyber incidents that lead to a covered claim, including—

"(A) identification of the affected databases, information systems, or devices that were, or are reasonably believed to have been, accessed by an unauthorized person;

"(B) a description of the vulnerabilities, tactics, techniques, and procedures used;

"(C) any identifying information related to the malicious actors who perpetrated the incident;

"(D) documentation of cybersecurity policies put in place by the victim organization, including relevant cybersecurity controls;

"(E) a description of the network security of the victim of the cyber incident during the course of the cyber incident, including the state of implementation of commonly used cybersecurity controls;

"(F) the amount of the claim paid and any additional information about the scope of damage of the incident; and

"(G) the industrial sectors, regions, and number of employees of affected entities without providing any information that can reasonably be expected to identify such entities.

"(3) REGULATORY USE.—Information disclosed to the Bureau under this subsection that is not otherwise available, shall not be used by the Federal Government or any State, local,

Tribal, or territorial government to sanction or otherwise punish the entity disclosing the information, or the entity in which the cyber incident initially occurred.

"(4) PRESERVATION OF PRIVILEGE.—Disclosure of information pursuant to this subsection or by a covered entity to the Bureau shall not waive any otherwise applicable privilege, immunity, or protection provided by law.

"(5) PRESERVATION OF EXISTING OBLIGATIONS.—Nothing in this subsection shall modify, prevent, or abrogate any notice or notification obligations under Federal contracts, enforceable agreements with the Government, or other Federal law.

"(6) EXPECTATION OF DUE DILIGENCE FOR COVERED ENTITIES.—Covered entities shall take necessary steps to ensure that the data and information submitted to the Bureau is accurate.

"(7) ENFORCEMENT.—

"(A) RULEMAKING.—Not later than 270 days after the date of the enactment of this section, the Secretary, acting through the Executive Assistant Director, shall, after a 90-day comment period, publish in the Federal Register, an interim final rule implementing this subsection.

"(B) EFFECTIVE DATE.—Notwithstanding section 553 of title 5, United States Code, the rule published under subparagraph (A) shall be effective, on an interim basis, immediately upon publication, but may be subject to change and revision after public notice and opportunity for comment.

"(C) FINALIZATION OF RULE.—The Secretary shall finalize the rule published under subparagraph (A) not later than 1 year after publication of the interim final rule.

"(D) CONTENTS.—The rule under this paragraph shall—

"(i) require covered entities to submit a report every 90 days containing the data and information published pursuant to paragraph (2); and

"(ii) establish penalties, including fines of not more than $1,000,000 for any person who omits or fails to do any act, matter, or thing in this subsection required to be done, or causes or suffers such omission or failure.

"(g) Protection of Information.—

"(1) IN GENERAL.—No officer or employee of the Federal Government or agent of the Federal Government may, without the consent of the individual, entity, agency, or other person who is the subject of the submission or provides the submission—

"(A) use any submission that is furnished for exclusively statistical purposes under this section for any purpose other than the statistical purposes for which the submission is furnished;

"(B) make any publication or media transmittal of the data contained in a submission described in subparagraph (A) that permits information concerning individual entities or individual incidents to be reasonably inferred by either direct or indirect means; or

"(C) permit anyone other than a sworn officer, employee, agent, or contractor of the Bureau to examine an individual submission described in subsection (f).

"(2) IMMUNITY FROM LEGAL PROCESS.—Any submission (including any data derived from the submission) that is collected and retained by the Bureau, or an officer, employee, agent, or contractor of the Bureau, for exclusively statistical purposes under this section shall be immune from the legal process and shall not, without the consent of the individual, entity, agency, or other person who is the subject of the submission or provides the submission, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.

"(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to provide immunity from the legal process for a submission (including any data derived from the submission) if the submission is in the possession of any person, agency, or entity other than the Bureau or an officers, employee, agent, or contractor of the Bureau, or if the submission is independently collected, retained, or produced for purposes other than the purposes of this section.

"(h) Authorization of Appropriation.—There are authorized to be appropriated such sums as may be necessary to carry out this section. Such funds shall remain available until expended.".

(b) Technical and Conforming Amendment.—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 inserting after the item relating to section 2220A, as added by section 101 of this Act, the following:

"Sec.2220B.Bureau of Cyber Statistics.".