SEC. 101. PURPOSE. To codify mechanisms for enabling cybersecurity information sharing between private and government entities, as well as among private entities, to better protect information systems and more effectively respond to cybersecurity incidents.

SEC. 102. DEFINITIONS.

(a) In this Act:

(1) CYBER THREAT- The term `cyber threat' means any action that may result in unauthorized access in order to damage or impair the integrity, confidentiality, or availability of an information system or unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system, except that exceeding authorized access of an information system shall not be considered a cyber threat if such access solely involves a violation of consumer terms of service or consumer licensing agreements.

(2) CYBER THREAT INDICATOR- The term `cyber threat indicator' means information—

(A) that is necessary to indicate, describe or identify —

(i) malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat;
(ii) a method of defeating a technical or operational control;
(iii) a technical vulnerability;
(iv) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system inadvertently to enable the defeat of a technical control or an operational control;
(v) malicious cyber command and control;
(vi) any combination of (i)-(v).

(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat.

(3) FEDERAL ENTITY- The term `Federal entity' means an agency or department of the United States, or any component, officer, employee, or agent of such an agency or department acting in his or her official capacity.

(4) GOVERNMENTAL ENTITY- The term `governmental entity' means any Federal entity and agency or department of a State, local, tribal, or territorial government, or any component, officer, employee, or agent of such an agency or department, acting in his or her official capacity.

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION – The term ‘Information sharing and analysis organization’ means an information sharing and analysis organization as defined in Section 212 of the Homeland Security Act of 2002.

(6) INFORMATION SYSTEM- The term `information system' means a discrete set of hardware and software information resources that collects, processes, maintains, uses, shares, disseminates, or disposes of information and communications.

(7) MALICIOUS CYBER COMMAND AND CONTROL- The term `malicious cyber command and control' means a method for remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system, that is known or reasonably suspected of being associated with a known or suspected cyber threat.

(8) MALICIOUS RECONNAISSANCE- The term `malicious reconnaissance' means a method for probing or monitoring an information system for the purpose of discerning technical vulnerabilities of the information system, if such method is known or reasonably suspected of being associated with a known or suspected cyber threat.

(9) NON-FEDERAL ENTITY- The term `non-Federal entity' means a private entity or a governmental entity other than a Federal entity.

(10) OPERATIONAL CONTROL- The term `operational control' means a security control for an information system that primarily is implemented and executed by people.

(11) PRIVATE ENTITY- The term `private entity' has the meaning given the term `person' in section 1 of title 1, United States Code, and does not include a governmental entity, or a foreign government or any component thereof.

(12) SECTOR SPECIFIC AGENCY - The term ‘sector-specific agency’ has the meaning given such term in the Cybersecurity Enhancement Act of 2014, P.L. 113-274.

(13) TECHNICAL CONTROL- The term `technical control' means a hardware or software restriction on, or audit of, access or use of an information system or information that is stored on, processed by, or transiting an information system that is intended to ensure the confidentiality, integrity, or availability of that information system or the information processed or stored by that information system.

(14) TECHNICAL VULNERABILITY- The term `technical vulnerability' means any attribute of hardware, firmware or software that could enable or facilitate the defeat of a technical control.

SEC. 103. AUTHORIZATION TO PROVIDE CYBER THREAT INDICATORS

(a) Voluntary Sharing of Cyber Threat Indicators – Notwithstanding any other provision of law, any private entity may disclose lawfully obtained cyber threat indicators to private information sharing and analysis organizations, and the National Cybersecurity and Communications Integration Center, consistent with this Act.

(b) Voluntary Sharing with Law Enforcement - Any entity may disclose lawfully obtained cyber threat indicators to a Federal entity for investigative purposes consistent with its lawful authorities.

(c) Use and Protection of Information- A private entity disclosing or receiving cyber threat indicators pursuant to this section—

(1) may use, retain, or further disclose such cyber threat indicators solely for the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from cyber threats or identifying or mitigating such threats, or for reporting a crime;

(2) shall take reasonable efforts to minimize information that can be used to identify specific persons and is reasonably believed to be unrelated to a cyber threat; and to safeguard information that can be used to identify specific persons from unintended disclosure and unauthorized access or acquisition; and

(3) shall comply with reasonable restrictions that a private entity places on the subsequent disclosure or retention of cyber threat indicators that it discloses to other private entities.

SEC. 104. PRIVATE INFORMATION SHARING AND ANALYSIS ORGANIZATIONS.

(a) Standards Organization – The Secretary of Homeland Security, in consultation with the Secretary of Commerce, the Attorney General, the Director of the Office of Management and Budget, the heads of sector-specific agencies and other appropriate Federal agencies, shall through an open and competitive process, select a private entity to identify, or develop if necessary, through an open and consultative process, a common set of best practices for the creation and operation of private information sharing and analysis organizations.

SEC. 105. CIVILIAN CYBER THREAT INDICATOR PORTAL.

(a) Civilian Portal - The Secretary of Homeland Security shall designate the National Cybersecurity and Communications Integration Center to receive and distribute cyber threat indicators in as close to real time as practicable, consistent with, and in accordance with the purposes of, this Act.

(b) Sharing With Federal Agencies- The Secretary of Homeland Security, in coordination with the Attorney General, and in consultation with the Director of the Office of Management Budget, the Director of National Intelligence, the Secretary of Defense, the heads of sector-specific agencies and other appropriate Federal agencies, shall ensure that cyber threat indicators received and disclosed by the National Cybersecurity and Communications Integration Center are shared with other Federal entities in as close to real time as practicable, consistent with, and in accordance with the purposes of, this Act.

(c) Real-Time Sharing - The Secretary of Homeland Security, in coordination with Director of the National Institute for Standards and Technology, and consistent with the Cybersecurity Enhancement Act of 2014, P.L. 113-274, shall develop a program that supports and rapidly advances the development, adoption and implementation of automated mechanisms for the real

time sharing of cyber threat indicators. To the maximum extent feasible, the Secretary will ensure that the program relies on open source software development best practices.

SEC 106. LIMITATION OF LIABILITY.

(a) Liability for Disclosure of Cyber Threat Indicators - No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any entity for the voluntary disclosure or receipt of a lawfully obtained cyber threat indicator consistent with the requirements of this Act, and that the entity was not otherwise required to disclose, to or from-

(1) the National Cybersecurity and Communications Integration Center, pursuant to Section 105; or

(2) a private information sharing and analysis organization, provided such organization maintains a publicly-available self-certification that it has adopted the best practices in accordance with those identified or developed pursuant to Section 104.

(b) Protection From Public Disclosure- Any cyber threat indicator disclosed by a non-Federal entity to the National Cybersecurity and Communications Integration Center, shall be--

(1)exempt from disclosure under section 552(b)(3) of title 5, United States Code, section 552a(d) of title 5, United States Code, or any State law otherwise requiring disclosure; and

(2) treated as voluntarily shared information under section 552 of title 5, United States Code, or any State law otherwise requiring disclosure.

(c) Limitation of regulatory enforcement actions –

(1) No Federal entity may use a cyber threat indicator received pursuant to this Act as evidence in a regulatory enforcement action against an entity that disclosed such cyber threat indicator to the Federal government, consistent with Section 105.

(2) Nothing in this subsection shall be construed to prevent a Federal entity from using a cyber threat indicator received independently through other lawful means in a regulatory enforcement action, even if such cyber threat indicator is also received pursuant to this Act.

(d) Nothing in this section permits the otherwise unauthorized disclosure by a private entity of information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation to require protection against unauthorized disclosure for reasons of national defense or foreign relations of the United States; any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954; information related to intelligence sources and methods; or information that is specifically subject to a court order or a certification, directive, or other authority precluding such disclosure.

SEC. 107. PRIVACY PROTECTONS.

(a) Privacy and Civil Liberties – The Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the Chief Privacy and Civil Liberties Officers at the Department of Homeland Security and Department of Justice, the Secretary of Commerce, the Director of National Intelligence, the Secretary of Defense, the Director of the Office of Management and Budget, the heads of sector-specific agencies and other appropriate agencies, and the Privacy and Civil Liberties Oversight Board, shall develop and periodically review policies and procedures governing the receipt, retention, use, and disclosure of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this Act. Such policies and procedures shall—

(1) reasonably limit the acquisition, interception, retention, use and disclosure of cyber threat indicators that are reasonably likely to identify specific persons, consistent with the need to carry out the responsibilities of this Act, including by-

(A) establishing a process for the timely destruction of information that is known not to be directly related to a purpose or use authorized under the Act;

(B) establishing a process to anonymize and safeguard information received and disclosed, that can be used to identify specific persons unrelated to a cyber threat;

(2) establish guidelines, which shall be made public, to permit law enforcement use of cyber threat indicators received by a governmental entity pursuant to Section 105, only to investigate, prosecute, disrupt, or otherwise respond to-

(A) a computer crime;
(B) a threat of death or serious bodily harm;
(C) a serious threat to a minor, including sexual exploitation and threats to physical safety; or
(D) an attempt or conspiracy to commit an offense described in (A) – (C).

(3) preserve the confidentiality of disclosed proprietary information to the greatest extent practicable, and require recipients of such information to be informed that the cyber threat indicators disclosed may only be used for the purposes authorized in this Act; and

(4) provide for appropriate penalties for any officer, employee, or agent of an agency or department who violates the restrictions under this Act with respect to receipt, retention or disclosure of cyber threat indicators.

(b) The head of each agency that receives or discloses cyber threat indicators pursuant to this Act shall establish a program to monitor and oversee compliance with the policies and procedures issued under this section.

(c) The policies and procedures under this section shall be provided to the appropriate Committees of Congress, and to the maximum extent practicable, shall be posted on the Internet website of such agency.

(d) On an annual basis, the Chief Privacy and Civil Liberties Officers of the Department of Justice and the Department of Homeland Security, in consultation with the privacy and civil liberties officers of appropriate agencies, shall submit a joint report to the Congress assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this Act.

SEC. 108. CONSTRUCTION AND FEDERAL PREEMPTION.

(a) Construction- Nothing in this Act may be construed--

(1) to limit any law or regulation that requires the disclosure, receipt or retention of information;

(2) to limit an entity's authority to share information concerning potential criminal activity or investigations with law enforcement entities;

(3) to limit or prohibit otherwise lawful disclosures of information by a private entity to any governmental or private entity not conducted under this Act;

(4) to permit the otherwise unauthorized disclosure by a private entity of information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation to require protection against unauthorized disclosure for reasons of national defense or foreign relations of the United States; any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954; information related to intelligence sources and methods; or information that is specifically subject to a court order or a certification, directive, or other authority precluding such disclosure;

(5) to authorize or limit liability for actions that would violate the regulations adopted by the Federal Communications Commission on preserving the open Internet, or any successor regulations thereto, nor to modify or alter the obligations of private entities under such regulations; or

(6) to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(b) Federal Preemption- This Act supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the retention, use or disclosure of cyber threat indicators by private entities to the extent such law contains requirements inconsistent with this Act.

(c) Preservation of Other State Law- Except as expressly provided, nothing in this Act shall be construed to preempt the applicability of any other State law or requirement.

(d) No Creation of a Right to Information- The provision of information to a non-Federal entity under this Act does not create a right or benefit to similar information by any other non-Federal entity.

(e) No Waiver of Privilege - No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this Act shall lose its privileged character.

(f) Prohibition on Requirement to Provide Information to the Federal Government- Nothing in this Act may be construed to permit a Federal entity--

(1) to require a non-Federal entity to share information with the Federal Government;

(2) to condition the disclosure of cyber threat indicators pursuant to this Act to a non-Federal entity on the provision of cyber threat information to the Federal Government; or

(3) to condition the award of any Federal grant, contract or purchase on the provision of cyber threat indicators to a Federal entity, if the provision of such indicators does not reasonably relate to the protection of the Federal entity's information system or information, goods, or services covered by the award.